BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 132 828 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 158(3) EPC

(43) Date of publication:
12.09.2001 Bulletin 2001/37

(21) Application number: **00961019.7**

(22) Date of filing: **14.09.2000**

(51) Int Cl.[7]: **G06F 15/00**, G10K 15/02

(86) International application number:
PCT/JP00/06308

(87) International publication number:
WO 01/22242 (29.03.2001 Gazette 2001/13)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **17.09.1999 JP 30972199**
17.09.1999 JP 30972299

(71) Applicant: **Sony Corporation**
Tokyo 141-0001 (JP)

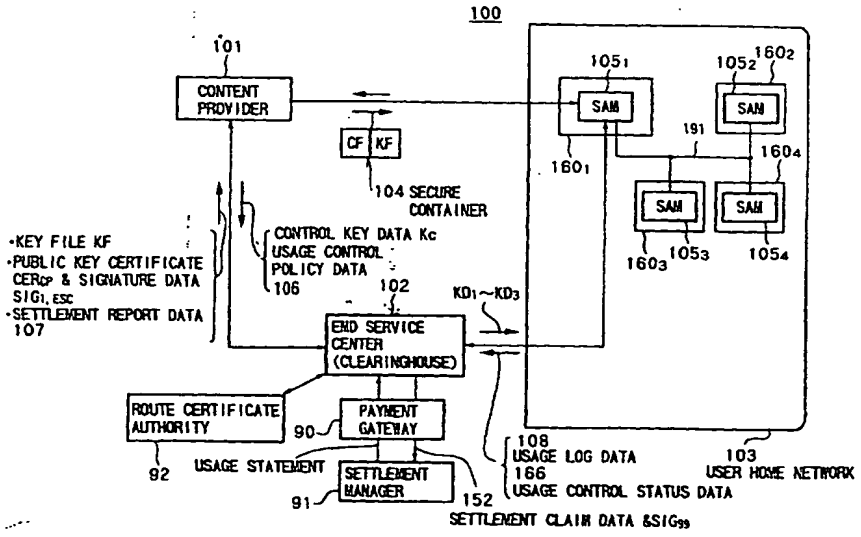
(72) Inventors:
- **NONAKA, Akira Sony Corporation**
Tokyo 141-0001 (JP)
- **EZAKI, Tadashi Sony Corporation**
Tokyo 141-0001 (JP)

(74) Representative: **Körber, Martin, Dipl.-Phys.**
Mitscherlich & Partner
Patentanwälte
Sonnenstrasse 33
80331 München (DE)

(54) DATA PROVIDING SYSTEM AND METHOD THEREFOR

(57) To provide a data providing system able to protect the interests of interested parties of a data providing apparatus. The content provider 101 distributes a secure container 104 storing content data encrypted using content key data, content key data encrypted using distribution key data, and encrypted usage control policy data showing handling of the content data to a SAM 105_1 of a user home network 103. The SAM 105_1 etc. decrypts the content key data and usage control policy data stored in the secure container 104 and determines the handling such as the purchase form and usage form of the content data based on the decrypted usage control policy data.

FIG.1



EP 1 132 828 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to a data providing system providing content data and a method of same, a data providing apparatus, and a data processing apparatus.

BACKGROUND ART

[0002] There is a data providing system for distributing encrypted content data to data processing apparatuses of users concluding predetermined contracts and having the related data processing apparatuses decrypt and reproduce and record the content data.

[0003] As one of such data providing systems, there is the conventional EMD (electronic music distribution) system for distributing music data.

[0004] Figure 145 is a view of the configuration of a conventional EMD system 700.

[0005] In the EMD system 700 shown in Fig. 145, content providers 701a and 701b encrypt content data 704a, 704b, and 704c and copyright information 705a, 705b, and 705c by session key data obtained after mutual certification and supply them to a service provider 710 on-line or supply by off-line. Here, the copyright information 705a, 705b, and 705c include for example SCMS (serial copy management system) information, electronic watermark information requesting burying in the content data, and information concerning the copyright requesting burying in a transmission protocol of the service provider 710.

[0006] The service provider 710 decrypts the received content data 704a, 704b, and 704c and copyright information 705a, 705b, and 705c by using the session key data.

[0007] Then, the service provider 710 buries the copyright information 705a, 705b, and 705c in the content data 704a, 704b, and 704c decrypted or received offline to produce content data 707a, 707b, and 707c. At this time, the service provider 710 changes predetermined frequency domains of for example the electronic watermark information among the copyright information 705a, 705b, and 705c and buries them in the content data 704a, 704b, and 704c and buries the SCMS information in a network protocol used when transmitting the related content data to the user.

[0008] Further, the service provider 710 encrypts the content data 707a, 707b, and 707c by using content key data Kca, Kcb, and Kcc read out from a key database 706. Thereafter, the service provider 710 encrypts a secure container 722 storing the encrypted content data 707a, 707b, and 707c by the session key data obtained after the mutual certification and transmits the same to a CA (conditional access) module 711 existing in a terminal 709 of the user.

[0009] The CA module 711 decrypts the secure container 722 by using the session key data. Also, the CA module 711 receives the content key data Kca, Kcb, and Kcc from the key database 706 of the service provider 710 by using a charge function such as an electronic settlement and CA and decrypts them by using the session key data. By this, in the terminal 709, it becomes possible to decrypt the content data 707a, 707b, and 707c by using the content key data Kca, Kcb, and Kcc.

[0010] At this time, the CA module 711 performs charge processing in units of content, produces charge information 721 in accordance with a result of this, and encrypts this by the session key data and then transmits the same to a right clearing module 720 of the service provider 710.

[0011] In this case, the CA module 711 collects items to be managed by the service provider 710 concerning services provided by itself, that is, the contract (update) information and the monthly basic fee and other network rent of the users, performs the charge processing in units of the content, and ensure security of a physical layer of the network.

[0012] The service provider 710 performs distributes profit among the service provider 710 and the content providers 701a, 701b, and 701c when receiving the charge information 721 from the CA module 711.

[0013] At this time, the profit is distributed from the service provider 710 to the content providers 701a, 701b, and 701c via for example the JASRAC (Japanese Society for Rights of Authors, Composers, and Publishers). Also, the profit of the content provider is distributed to copyright owner, an artist, a song writer, and/or composer of the related content data and their affiliated production companies by the JASRAC.

[0014] Also, in the terminal 709, when recording the content data 707a, 707b, and 707c decrypted by using the content key data Kca, Kcb, and Kcc in a RAM type storage medium 723 or the like, copying is controlled by rewriting SCMS bits of the copyright information 705a, 705b, and 705c. Namely, on the user side, copying is controlled based on the SCMS bits buried in the content data 707a, 707b, and 707c to achieve protection of the copyright.

[0015] The SCMS prohibits copying of the content data over for example two generations. Copying of one generation can be carried out without restriction, however, so there is a problem of insufficient protection of the copyright owner.

[0016] Also, in the EMD system 700, the content data not encrypted by the service provider 710 can be technically freely handled, so interested parties of the content provider 710 must monitor actions etc. of the service provider 710, so there are problems in that the load of the related monitoring is large and, at the same time, there is a high possibility of improper loss of the profit of the content provider 701.

[0017] Also, in the EMD system 700, it is difficult to restrict acts of the terminal 709 of the user authoring the content data distributed from the service provider 710

and redistributing the same to another terminal etc., so there is the problem of the improper loss of the profit of the content provider 701.

DISCLOSURE THE INVENTION

[0018] The present invention was made in consideration with the problems of the related art mentioned above and has as an object thereof to provide a data providing system capable of adequately protecting the profit of right holders (interested parties) of the content provider and a method of the same.

[0019] Also, another object of the present invention is to provide a data providing system capable of reducing the load of inspection for protecting the profit of the right holders of the content provider and a method of the same.

[0020] To solve the problems of the prior art mentioned above and achieve the above objects, a data providing system of a first aspect of the present invention is preferably a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus provides the content data encrypted by using the content key data, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the key file and determines the handling of the content data based on the related decrypted usage control policy data.

[0021] The mode of operation of the data providing system of the first aspect of the present invention becomes as follows.

[0022] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

[0023] Then, the content data encrypted by using the content key data is provided from the data providing apparatus to the data processing apparatus.

[0024] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the key file are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0025] Also, a data providing system of a second aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus distributes a module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0026] The mode of operation of the data providing system of the second aspect of the present invention becomes as follows.

[0027] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced.

[0028] Then, the related produced key file is distributed from the management apparatus to the data providing apparatus.

[0029] Then, the module storing the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus.

[0030] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0031] A data providing system of a third aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus distributes a module storing a content file containing content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0032] The mode of operation of the data providing system of the third aspect of the present invention becomes as follows.

[0033] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data providing apparatus.

[0034] Then, the module storing the content file containing the content data encrypted by using the content

key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus.

[0035] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0036] Also, a data providing system of a fourth aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus individually distributes the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0037] The mode of operation of the data providing system of the fourth aspect of the present invention becomes as follows.

[0038] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data providing apparatus.

[0039] Then, in the data providing apparatus, the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus are distributed.

[0040] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

[0041] Also, a data providing system of a fifth aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus distributes a content file storing the content data encrypted by using the content key data to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0042] The mode of operation of the data providing system of the fifth aspect of the present invention becomes as follows.

[0043] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced.

[0044] The related produced key file is distributed from the management apparatus to the data processing apparatus.

[0045] Also, the content file storing the content data encrypted by using the content key data is distributed from the data providing apparatus to the data processing apparatus.

[0046] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

[0047] Also, a data providing system of a sixth aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus distributes a module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0048] The mode of operation of the data providing system of the sixth aspect of the present invention becomes as follows.

[0049] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data providing apparatus.

[0050] Then, the module storing the content data encrypted by using the content key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus.

[0051] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the

handling of the content data is determined based on the related decrypted usage control policy data.

[0052] Also, a data providing system of a seventh aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0053] The mode of operation of the data providing system of the seventh aspect of the present invention becomes as follows.

[0054] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data providing apparatus.

[0055] Then, the content data encrypted by using the content key data and the key file received from the management apparatus are individually distributed from the data providing apparatus to the data processing apparatus.

[0056] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

[0057] Also, a data providing system of an eighth aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data and distributes the related produced key file to the data processing apparatus, the data processing apparatus distributes the content data encrypted by using the content key data to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0058] The mode of operation of the data providing system of the eighth aspect of the present invention becomes as follows.

[0059] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data processing apparatus.

[0060] Also, the content data encrypted by using the content key data are distributed from the data providing apparatus to the data processing apparatus.

[0061] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

[0062] Also, a data providing system of a ninth aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the content key data, the encrypted content key data received from the management apparatus, and the encrypted usage control policy data to the data processing apparatus, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0063] The mode of operation of the data providing system of the ninth aspect of the present invention becomes as follows.

[0064] In the management apparatus, the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data are produced, and they are sent to the data providing apparatus.

[0065] Then, the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus are individually distributed from the data providing apparatus to the data processing apparatus.

[0066] Then, in the data processing apparatus, the distributed content key data and the usage control policy data are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

[0067] Also, a data providing system of a 10th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing ap-

paratus by a management apparatus, wherein the management apparatus produces encrypted content key data and encrypted usage control policy data indicating handling of the content data and distributes the same to the data processing apparatus, the data providing apparatus distributes the content data encrypted by using the content key data to the data processing apparatus, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0068] The mode of operation of the data providing system of the 10th aspect of the present invention becomes as follows.

[0069] In the management apparatus, the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data are produced, and they are sent to the data processing apparatus.

[0070] Also, the content data encrypted by using the content key data are distributed from the data providing apparatus to the data processing apparatus.

[0071] Then, in the data processing apparatus, the distributed content key data and the usage control policy data are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

[0072] Also, a data providing system of an 11th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a data processing apparatus, and a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides the content data encrypted by using the content key data, the data distribution apparatus distributes the provided content data to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0073] The mode of operation of the data providing system of the 11th aspect of the present invention becomes as follows.

[0074] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced.

[0075] Then, the content data encrypted by using the content key data is provided from the data providing apparatus to the data distribution apparatus.

[0076] Then, the provided content data is distributed from the data distribution apparatus to the data processing apparatus.

[0077] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the key file are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

[0078] Also, a data providing system of a 12th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0079] The mode of operation of the data providing system of the 12th aspect of the present invention becomes as follows.

[0080] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data providing apparatus.

[0081] Then, the first module storing the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus is provided from the data providing apparatus to the data distribution apparatus.

[0082] Then, the second module storing the provided content file and the key file is distributed from the data distribution apparatus to the data processing apparatus.

[0083] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed second module are decrypted, and the handling of the content data stored in the distributed second module is determined based on the related decrypted usage control policy data.

[0084] Also, a data providing system of a 13th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus,

wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file containing the content data encrypted by using the content key data and a key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0085] Also, a data providing system of a 14th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content file and key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0086] Also, a data providing system of a 15th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus provides a content file storing the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0087] Also, a data providing system of a 16th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content data and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0088] Also, a data providing system of a 17th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content data and the key file to the data distribution apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0089] Also, a data providing system of an 18th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data processing apparatus provides the content data encrypted by using the con-

tent key data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0090] Also, a data providing system of a 19th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus provides encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data providing apparatus, the data providing apparatus individually distributes the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content data, the encrypted content key data, and the encrypted usage control policy data to the data distribution apparatus, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0091] Also, a data providing system of a 20th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus provides encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus, the data providing apparatus provides the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, and the data processing apparatus decrypts the distribute the content key data and the usage control policy data and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0092] Also, a data providing system of a 21st aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file and the key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0093] Also, a data providing system of a 22nd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file to the data distribution apparatus, provides the key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0094] Also, a data providing system of a 23rd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file provided from the data providing apparatus and the produced key file to the data distribution apparatus, the data distribution appa-

ratus distributes the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0095] Also, a data providing system of a 24th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, provides the content file provided from the data providing apparatus to the data distribution apparatus, and provides the produced key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0096] Also, a data providing system of a 25th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file and a key file provided from the management apparatus in the database device, the management apparatus produces the key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes the content file and key file obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0097] Also, a data providing system of a 26th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces the key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data distribution apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0098] Also, a data providing system of a 27th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces the key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data processing apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0099] Also, a data providing system of a 28th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files and key files provided from corresponding management apparatuses in the database device, the management apparatuses produce key files storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and provide the related produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus, and the data processing appara-

tus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0100] Also, a data providing system of a 29th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and provide the related produced key files to the data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0101] Also, a data providing system of a 30th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0102] Also, a data providing system of a 31st aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce the content files storing the related encrypted content data, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced content files and the produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0103] Also, a data providing system of a 32nd aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses, and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce the content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced key files to corresponding data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatuses to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0104] Also, a data providing system of a 33rd aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received

from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce the content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatuses to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0105] Also, a data providing method of a first aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides the content data encrypted by using the content key data, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the key file and determines the handling of the content data based on the related decrypted usage control policy data.

[0106] Also, a data providing method of a second aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the produced key file from the management apparatus to the data providing apparatus, distributing a module storing a content file storing the content data encrypted by using the content key data and the key file distributed from the management apparatus from the data providing apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

[0107] Also, a data providing method of a third aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, distributing a module storing a content file containing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

[0108] Also, a data providing method of a fourth aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related key file from the management apparatus to the data providing apparatus, individually distributing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus from the data providing apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0109] Also, a data providing method of a fifth aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related key file from the management apparatus to the data processing apparatus, distributing a content file storing the content data encrypted by using the content key data from the data providing apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0110] Also, a data providing method of a sixth aspect

of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, distributing a module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

[0111] Also, a data providing method of a seventh aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0112] Also, a data providing method of an eighth aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file to the data processing apparatus, in the data providing apparatus, distributing the content data encrypted by using the content key data to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0113] Also, a data providing method of a ninth aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0114] Also, a data providing method of a 10th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributing the same to the data processing apparatus, in the data providing apparatus, distributing the content data encrypted by using the content key data to the data processing apparatus, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0115] Also, a data providing method of an 11th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a data processing apparatus, and a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, providing the content data encrypted by using the content key data from the data providing apparatus to the data distribution apparatus, in the data distribution apparatus, distributing the provided content data to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0116] Also, a data providing method of a 12th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data

and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data providing apparatus, providing a first module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus from the data providing apparatus to the data distribution apparatus, and distributing a second module storing the provided content file and the key file from the data distribution apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0117] Also, a data providing method of a 13th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, providing a first module storing a content file containing the content data encrypted by using the content key data and a key file received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, distributing a second module storing the provided content file to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0118] Also, a data providing method of a 14th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the produced key file from the management apparatus to the data providing apparatus, individually distributing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus from the data providing apparatus to the data distribution apparatus, individually distributing the distributed content file and the key file from the data distribution apparatus to the data distribution apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0119] Also, a data providing method of a 15th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data processing apparatus, providing a content file storing the content data encrypted by using the content key data from the data providing apparatus to the data distribution apparatus, and distributing the provided content file from the data distribution apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0120] Also, a data providing method of a 16th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, providing a first module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, distributing a second module storing the provided content data and the key file to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0121] Also, a data providing method of a 17th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data

processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, individually distributing the distributed content data and the key file to the data distribution apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0122] Also, a data providing method of an 18th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributing the related produced key file to the data processing apparatus, in the data providing apparatus, providing the content data encrypted by using the content key data to the data distribution apparatus, in the data distribution apparatus, distributing the provided content data to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0123] Also, a data providing method of a 19th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, providing encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data providing apparatus, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data which are received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, individually distributing the distributed content data, the encrypted content key data, and the encrypted usage control policy data to the data distribution apparatus, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0124] Also, a data providing method of a 20th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, distributing encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus, in the data providing apparatus, distributing the content data encrypted by using the content key data to the data distribution apparatus, in the data distribution apparatus, distributing the provided content data to the data processing apparatus, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0125] Also, a data providing method of a 21st aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file and the key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0126] Also, a data providing method of a 22nd aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the

provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file to the data distribution apparatus and provides the key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0127] Also, a data providing method of a 23rd aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, provides the content file provided from the data providing apparatus and the produced key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0128] Also, a data providing method of a 24th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, provides the content file provided from the data providing apparatus to the data distribution apparatus, and provides the produced key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0129] Also, a data providing method of a 25th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file and a key file provided from the management apparatus in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes the content file and key file obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0130] Also, a data providing method of a 26th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data distribution apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0131] Also, a data providing method of a 27th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the

related produced key file to the data processing apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0132] Also, a data providing method of a 28th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files and key files provided from corresponding management apparatuses in the database device, the management apparatuses produce the key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0133] Also, a data providing method of a 29th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce the key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatuses to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0134] Also, a data providing method of a 30th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce the key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0135] Also, a data providing method of a 31st aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced content files and the produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0136] Also, a data providing method of a 32nd aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding man-

agement apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the related produced key files to corresponding data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and key files provided from the management apparatuses to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0137] Also, a data providing method of a 33rd aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0138] Also, a data providing system of a 34th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus, wherein the data providing apparatus distributes a module storing the content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus by using a predetermined communication protocol in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0139] The mode of operation of the data providing system of the 34th aspect of the present invention becomes as follows.

[0140] The module storing the content data encrypted by using the content key data, the encrypted content key data, and the encrypted usage control policy data indicating the handling of the content data is distributed from the data providing apparatus to the data processing apparatus.

[0141] At this time, the related module is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0142] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0143] In this way, by storing the usage control policy data indicating the handling of the related content data in the module storing the content data, in the data processing apparatus, it becomes possible to handle (use) the content data based on the usage control policy data produced by the interested parties of the data providing apparatus.

[0144] Also, the module is distributed from the data providing apparatus to the data processing apparatus in the format not depending upon a predetermined communication protocol, so a compression method, encryption method, etc. of the content data stored in the module can be freely determined by the data providing apparatus.

[0145] Also, in the data providing system of the 34th aspect of the present invention, preferably the module further storing signature data for verifying a legitimacy of a producer and a transmitter of at least one data among the content data, the content key data, and the usage control policy data is distributed to the data processing apparatus.

[0146] Also, in the data providing system of the 34th aspect of the present invention, preferably the data providing apparatus distributes the module further storing at least one data between data for verifying if the related data is not tampered with and signature data for verifying if the related data was normally certified by a predetermined manager for at least one data among the content data, the content key data, and the usage control policy data to the data processing apparatus.

[0147] Also, in the data providing system of the 34th aspect of the present invention, preferably the data processing apparatus determines a purchase form of the content data based on the usage control policy data, and where the content data is transferred to another data processing apparatus, the signature data indicating the legitimacy of the purchaser of the related content data and the signature data indicating the legitimacy of the transmitter of the related content data are made different.

[0148] A data providing system of 35th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus distributes a module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0149] The mode of operation of the data providing system of the 35th aspect of the present invention becomes as follows.

[0150] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced.

[0151] Then, the related produced key file is distributed from the management apparatus to the data providing apparatus.

[0152] Then, the module storing the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0153] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0154] Also, in the data providing system of the 35th aspect of the present invention, preferably the management apparatus produces signature data for verifying the legitimacy of the producer of the key file and produces the key file further storing the related signature data.

[0155] Also, in the data providing system of the 35th aspect of the present invention, preferably the data providing apparatus produces the content key data and the usage control policy data and transmits the same to the management apparatus, and the management apparatus produces the key file based on the received content key data and usage control policy data and registers the related produced key file.

[0156] Also, a data providing apparatus of the present invention is a data providing apparatus which is managed by a management apparatus and distributes content data to a data processing apparatus, receiving a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data from the management apparatus and distributing a module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus.

[0157] Also, a data processing apparatus of the present invention is a data processing apparatus managed by a management apparatus and utilizing content data, receiving a module containing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and a content file storing the content data encrypted by using the content key data, determining at least one between a purchase form and an usage form of the content data based on the usage control policy data, and transmitting a log data indicating the log of the determined at least one of the related purchase form and usage form to the management apparatus.

[0158] Also, a data providing system of a 36th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus distributes a module storing a content file containing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0159] The mode of operation of the data providing system of the 36th aspect of the present invention becomes as follows.

[0160] In the management apparatus, the key file

storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

[0161] Then, the module storing the content file containing the content data encrypted by using the content key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0162] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0163] Also, a data providing system of a 37th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0164] The mode of operation of the data providing system of the 37th aspect of the present invention becomes as follows. In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

[0165] Then, in the data processing apparatus, the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus are individually distributed to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0166] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

[0167] Also, a data providing system of a 38th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus distributes a content file storing the content data encrypted by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0168] Below, an explanation will be made of the mode of operation of the data providing system of the 38th aspect of the present invention.

[0169] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced.

[0170] The related produced key file is distributed from the management apparatus to the data processing apparatus.

[0171] Also, the content file storing the content data encrypted by using the content key data is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0172] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

[0173] Also, a data providing system of a 39th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus distributes a module storing the content data encrypted by using the content key data and the key file received from the management appara-

tus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0174] Below, an explanation will be made of the mode of operation of the data providing system of the 39th aspect of the present invention.

[0175] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

[0176] Then, the module storing the content data encrypted by using the content key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0177] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0178] Also, a data providing system of a 40th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0179] Below, an explanation will be made of the mode of operation of the data providing system of the 40th aspect of the present invention.

[0180] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

[0181] Then, the content data encrypted by using the content key data and the key file received from the management apparatus are individually distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0182] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

[0183] Also, a data providing system of a 41st aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus distributes the content data encrypted by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0184] Below, an explanation will be made of the mode of operation of the data providing system of the 41st aspect of the present invention.

[0185] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is distributed to the data processing apparatus.

[0186] Also, the content data encrypted by using the content key data is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0187] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

[0188] Also, a data providing system of a 42nd aspect of the present invention is a data providing system for

distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0189] Below, an explanation will be made of the mode of operation of the data providing system of the 42nd aspect of the present invention.

[0190] In the management apparatus, the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data are produced and are sent to the data providing apparatus.

[0191] Then, the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus are individually distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0192] Then, in the data processing apparatus, the distributed content key data and the usage control policy data are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

[0193] Also, a data providing system of a 43rd aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the same to the data processing apparatus, the data providing apparatus distributes the content data encrypted by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0194] Below, an explanation will be made of the mode of operation of the data providing system of the 43rd aspect of the present invention.

[0195] In the management apparatus, the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data are produced and are distributed to the data processing apparatus.

[0196] Then, the content data encrypted by using the content key data is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0197] Then, in the data processing apparatus, the distributed content key data and the usage control policy data are decrypted, and the handling of the distribution the content data is determined based on the related decrypted usage control policy data.

[0198] Also, a data providing system of a 44th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus provides a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data distribution apparatus, the data distribution apparatus distributes a second module storing the encrypted content data, content key data, and the usage control policy data stored in the provided first module to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data based on the related decrypted usage control policy data.

[0199] Below, an explanation will be made of the mode of operation of the data providing system of the 44th aspect of the present invention.

[0200] The first module storing the content data encrypted by using the content key data, the encrypted content key data, and the encrypted usage control policy data indicating the handling of the content data is provided from the data providing apparatus to the data distribution apparatus by for example using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0201] Next, the second module storing the encrypted content data, content key data, and the usage control policy data stored in the provided first module is distrib-

uted from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0202] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed second module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0203] In this way, by storing the usage control policy data indicating the handling of the related content data in the first module and second module storing the content data, in the data processing apparatus, it becomes possible to have the data processing apparatus perform the handling (usage) of the content data based on the usage control policy data produced by the interested parties of the data providing apparatus.

[0204] Also, the second module is distributed from the data distribution apparatus to the data processing apparatus in a format not depending upon on a predetermined communication protocol, so the compression method and encryption method etc. of the content data stored in the second module can be freely determined by the data providing apparatus.

[0205] A data providing system of a 45th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0206] Below, an explanation will be made of the mode of operation of the data providing system of the 45th aspect of the present invention.

[0207] In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

[0208] Then, the first module storing the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus is provided from the data providing apparatus to the data distribution apparatus.

[0209] Then, the second module storing the provided content file and the key file is distributed from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

[0210] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed second module are decrypted, and the handling of the content data stored in the distributed second module is determined based on the related decrypted usage control policy data.

[0211] A data providing system of a 46th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file containing the content data encrypted by using the content key data and a key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0212] Also, a data providing system of a 47th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a first data distribution apparatus and a second data distribution apparatus, distributing the content data from the first data distribution apparatus and the second data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the first data distribution apparatus, the second data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content

key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the first data distribution apparatus and the second data distribution apparatus, the first data distribution apparatus distributes a second module storing the provided content file and the key file to the data processing apparatus, the second data distribution apparatus distributes a third module storing the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and the third module and determines the handling of the content data based on the related decrypted usage control policy data.

[0213] Also, a data providing system of a 48th aspect of the present invention is a data providing system for providing first content data from a first data providing apparatus to a data distribution apparatus, providing second content data from a second data providing apparatus to the data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the first data providing apparatus, the second data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a first key file storing an encrypted first content key data and an encrypted first usage control policy data indicating the handling of the first content data and a second key file storing an encrypted second content key data and an encrypted second usage control policy data indicating the handling of the second content data, the first data providing apparatus provides a first module storing a first content file storing the first content data encrypted by using the first content key data and the first key file received from the management apparatus to the data distribution apparatus, the second data providing apparatus provides a second module storing a second content file storing the second content data encrypted by using the second content key data and the second key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a third module storing the provided first content file, the first key file, the second content file, and the second key file to the data processing apparatus, and the data processing apparatus decrypts the first content key data, the second content key data, the first usage control policy data, and the second usage control policy data stored in the distributed third module, determines the handling of the first content data based on the related decrypted first usage control policy data, and determines the handling of the second content data based on the related decrypted second usage control policy data.

[0214] Also, a data providing system of a 49th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0215] Also, a data providing system of a 50th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus distributes a content file storing the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0216] Also, a data providing system of a 51st aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file

storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content data and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0217] Also, a data providing system of a 52nd aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content data and the key file to the data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0218] Also, a data providing system of a 53rd aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data processing apparatus, and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus distributes the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0219] Also, a data providing system of a 54th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus provides encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data providing apparatus, the data providing apparatus individually distributes the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes the distributed content data, the encrypted content key data, and the encrypted usage control policy data to the data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0220] Also, a data providing system of a 55th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus provides encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus, the data providing apparatus provides the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributes the distributed provided content data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the distributed content data based on the related decrypted usage control policy data.

[0221] Also, a data providing system of a 56th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data,. produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file and the key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0222] Also, in the data providing system of the 56th aspect of the present invention, preferably the management apparatus produces a first module storing the content file and the key file and provides the related first module to the data distribution apparatus, and the data distribution apparatus produces a second module storing the content file and the key file stored in the first module and distributes the related second module to the data processing apparatus.

[0223] Also, in the data providing system of the 56th aspect of the present invention, preferably the management apparatus has at least one database among a database for storing and managing the content file, a database for storing and managing the key file, and a database for storing and managing the usage control policy data and centrally manages at least one among the content file, the key file, and the usage control policy data by using a content identifier uniquely allocated to the content data.

[0224] Also, a data providing system of a 57th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file to the data distribution apparatus and provides the key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0225] Also, a data providing system of a 58th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file provided from the data providing apparatus and the produced key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0226] Also, a data providing system of a 59th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, provides the content file provided from the data providing apparatus to the data distribution apparatus, and provides the produced key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related

communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0227] Also, a data providing system of a 60th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file and a key file provided from the management apparatus in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes the content file and key file obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0228] Also, a data providing system of a 61st aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0229] Also, a data providing system of a 62nd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data processing apparatus, the data distribution apparatus distributes the content file obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0230] Also, a data providing system of a 63rd aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files and key files provided from corresponding management apparatuses in the database device, the management apparatuses produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0231] Also, a data providing system of a 64th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content

files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatuses to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0232] Also, a data providing system of a 65th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0233] Also, a data providing system of a 66th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced content files and the produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0234] Also, a data providing system of a 67th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the related produced key files provided from the management apparatuses to corresponding data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and key files provided from the management apparatuses to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0235] Also, a data providing system of a 68th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding man-

agement apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the provided content files based on the related decrypted usage control policy data.

[0236] Also, a data providing system of a 69th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus provides a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data distribution apparatus, performs charge processing in units of the content data based on log data received from the data processing apparatus, and performs a profit distribution processing for distributing the profit paid by interested parties of the data processing apparatus to interested parties of the related data providing apparatus and interested parties of the data distribution apparatus, the data distribution apparatus distributes a second module storing the encrypted content data, content key data, and usage control policy data stored in the provided first module to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module, determines the handling of the content data based on the related decrypted usage control policy data, produces the log data for the handling of the related content data, and sends the related log data to the data providing apparatus.

[0237] Also, a data providing system of a 70th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, and a management apparatus, wherein the data providing apparatus provides content data, the data distribution apparatus distributes the content file provided from the data providing apparatus or a content file in accordance with the content data provided by the data providing apparatus provided from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the usage control policy data stored in a key file received from the data distribution apparatus or the management apparatus, determines the handling of the content data stored in the content file received from the data distribution apparatus or the management apparatus based on the related decrypted usage control policy data, and further distributes the content file and key file received from the data distribution apparatus or the management apparatus to the other data processing apparatus.

[0238] Also, a data providing method of a 34th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus, comprising the steps of distributing a module storing the content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

[0239] Also, a data providing method of a 35h aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the produced key file from the management apparatus to the data providing apparatus, and distributing a module storing a content file storing the content data encrypted by using the content key data and the key file distributed from the management apparatus from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

[0240] Also, a data providing method of a 36th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the

data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, distributing a module storing a content file containing the content data encrypted by using the content key data and a key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

[0241] Also, a data providing method of a 37th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data providing apparatus, and individually distributing a content file storing the content data encrypted by using the content key data and the key file distributed from the management apparatus from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0242] Also, a data providing method of a 38th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data processing apparatus, and distributing a content file storing the content data encrypted by using the content key data from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0243] Also, a data providing method of a 39th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, distributing a module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

[0244] Also, a data providing method of a 40th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0245] Also, a data providing method of a 41st aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributing the related produced key

file to the data processing apparatus, in the data providing apparatus, distributing the content data encrypted by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0246] Also, a data providing method of a 42nd aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0247] Also, a data providing method of a 43rd aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributing the same to the data processing apparatus, in the data providing apparatus, distributing the content data encrypted by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0248] Also, a data providing method of a 44th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, and a data processing apparatus, comprising the steps of providing a first module storing content data encrypted by using content key data, encrypted the content key data, and encrypted usage control policy data indicating the handling of the content data from the data providing apparatus to the data distribution apparatus, distributing a second module storing the encrypted content data, content key data, and the usage control policy data stored in the provided the first module from the data distribution apparatus to the data processing apparatus by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data based on the related decrypted usage control policy data.

[0249] Also, a data providing method of a 45th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data providing apparatus, providing a first module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus from the data providing apparatus to the data distribution apparatus, and distributing a second module storing the provided content file and the key file from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0250] Also, a data providing method of a 46th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus,

preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, providing a first module storing a content file containing the content data encrypted by using the content key data and a key file received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, distributing a second module storing the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0251] Also, a data providing method of a 47th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the produced key file from the management apparatus to the data providing apparatus, individually providing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus from the data providing apparatus to the data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and individually distributing the distributed content file and the key file from the data distribution apparatus to the data distribution apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0252] Also, a data providing method of a 48th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data processing apparatus, providing a content file storing the content data encrypted by using the content key data from the data providing apparatus to the data distribution apparatus, distributing the provided content file from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording. the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0253] Also, a data providing method of a 49th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, providing a first module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, distributing a second module storing the provided content data and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

[0254] Also, a data providing method of a 50th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, individually providing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, individually distributing the distributed content data and

the key file to the data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0255] Also, a data providing method of a 51st aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributing the related produced key file to the data processing apparatus, in the data providing apparatus, providing the content data encrypted by using the content key data to the data distribution apparatus, in the data distribution apparatus, distributing the provided content data to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0256] Also, a data providing method of a 52nd aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, providing encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data providing apparatus, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, individually distributing the distributed content data, the encrypted content key, data, and the encrypted usage control policy data to the data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0257] Also, a data providing method of a 53rd aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, distributing encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus, in the data providing apparatus, providing the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributing the provided content data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol by recording the same on a storage medium, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the related decrypted usage control policy data.

[0258] Also, a data providing method of a 54th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file and the key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0259] Also, a data providing method of a 55th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the

provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file to the data distribution apparatus and provides the key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0260] Also, a data providing method of a 56th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file provided from the data providing apparatus and the produced key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0261] Also, a data providing method of a 57th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, provides the content file provided from the data providing apparatus to the data distribution apparatus and provides the produced key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0262] Also, a data providing method of a 58th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file and a key file provided from the management apparatus in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes the content file and key file obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0263] Also, a data providing method of a 59th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data distribution apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed

key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0264] Also, a data providing method of a 60th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data processing apparatus, the data distribution apparatus distributes the content file obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

[0265] Also, a data providing method of a 61st aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files and key files provided from corresponding management apparatuses in the database device, the management apparatuses produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0266] Also, a data providing method of a 62nd aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatuses to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0267] Also, a data providing method of a 63rd aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0268] Also, a data providing method of a 64th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key

files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced content files and the produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0269] Also, a data providing method of a 65th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, send the related produced key files to corresponding data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatuses to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0270] Also, a data providing method of a 66th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

[0271] Also, a data providing method of a 67th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus provides a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data distribution apparatus, performs charge processing in units of the content data based on log data received from the data processing apparatus, performs profit distribution processing for distributing the profit paid by interested parties of the data processing apparatus to interested parties of the related data providing apparatus and interested parties of the data distribution apparatus, the data distribution apparatus distributes a second module storing the encrypted content data, content key data and usage control policy data stored in the provided first module to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module, determines the handling of the content data based on the related decrypted usage control policy data, produces the log data for the handling of the related content data and sends the related log data to the data providing apparatus.

[0272] Also, a data providing method of a 68th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution appara-

tus, a data processing apparatus, and a management apparatus, wherein the data providing apparatus provides content data, the data distribution apparatus distributes the content file provided from the data providing apparatus or a content file in accordance with the content data provided by the data providing apparatus received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the usage control policy data stored in the key file received from the data distribution apparatus or the management apparatus, determines the handling of the content data stored in the content file received from the data distribution apparatus or the management apparatus based on the related decrypted usage control policy data, and further distributes the content file and key file received from the data distribution apparatus or the management apparatus to the other data processing apparatus.

[0273] Also, a data providing system of a 71st aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus, wherein the data providing apparatus distributes a module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data in a format not depending upon at least one among existence of a compression of the content data, a compression method, a method of the encryption, and parameters of a signal giving the content data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0274] Also, a data providing system of a 72nd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus distributes a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data in a format not depending upon at least one among existence of compression of the content data, a compression method, a method of the encryption, and parameters of a signal giving the content data to the data distribution apparatus, the data distribution apparatus distributes a second module storing the encrypted content data, content key data, and the usage control policy data stored in the provided first module to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data based on the related decrypted usage control policy data.

[0275] Also, a data providing system of a 73rd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus distributes a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data distribution apparatus, the data distribution apparatus encrypts a plurality of second modules storing the encrypted content data, content key data, and the usage control policy data stored in the provided first module by using a common key obtained by mutual certification with the data processing apparatus, and then distributes the same to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol, and the data processing apparatus has a first processing circuit for decrypting the distributed plurality of second modules by using the common key, selecting a single or a plurality of second modules from among the related decrypted plurality of second modules, and performing charge processing with respect to a distribution service of the second modules and a tamper resistant second processing circuit receiving the selected the second modules, decrypting the content key data and the usage control policy data stored in the related second modules, and determining the handling of the content data based on the related decrypted usage control policy data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0276]

Fig. 1 is a view of the overall configuration of an EMD system of a first embodiment of the present invention,

Fig. 2 is a view for explaining a concept of a secure container of the present invention,

Fig. 3 is a functional block diagram of a content provider shown in Fig. 1 and a view of a flow of data related to data transmitted and received with a SAM of a user home network,

Fig. 4 is a functional block diagram of the content provider shown in Fig. 1 and a view of the flow of data related to the data transmitted and received between the content provider and an EMD service center,

Figs. 5A to 5C are views for explaining a format of the secure container transmitted from the content provider shown in Fig. 1 to the SAM,

Fig. 6 is a view for explaining data contained in a

content file shown in Fig. 5 in detail,
Fig. 7 is a view for explaining data contained in a key file shown in Fig. 5 in detail,
Fig. 8 is a view for explaining a header data stored in the content file,
Fig. 9 is a view for explaining a content ID,
Fig. 10 is a view for explaining a directory structure of the secure container,
Fig. 11 is a view for explaining a hyper link structure of the secure container,
Fig. 12 is a view for explaining a first example of ROM type storage medium used in the present embodiment,
Fig. 13 is a view for explaining a second example of the ROM type storage medium used in the present embodiment,
Fig. 14 is a view for explaining a third example of the ROM type storage medium used in the present embodiment,
Fig. 15 is a view for explaining a first example of RAM type storage medium used in the present embodiment,
Fig. 16 is a view for explaining a second example of the RAM type storage medium used in the present embodiment,
Fig. 17 is a view for explaining a third example of the RAM type storage medium used in the present embodiment,
Fig. 18 is a view for explaining a registration request use module transmitted from the content provider to the EMD service center,
Fig. 19 is a flowchart showing a routine of processing for registration from the content provider to the EMD service center,
Fig. 20 is a flowchart showing a routine of processing for preparation of an explanation in the content provider,
Fig. 21 is a flowchart showing a routine of processing for preparation of an explanation in the content provider,
Fig. 22 is a flowchart showing a routine of processing for preparation of an explanation in the content provider,
Fig. 23 is a functional block diagram of the EMD service center shown in Fig. 1 and a view of the flow of the data related to the data transmitted and received with the content provider,
Fig. 24 is a functional block diagram of the EMD service center shown in Fig. 1 and a view of the flow of the data related to the data transmitted and received between the SAM and a settlement manager shown in Fig. 1,
Fig. 25 is a view of the configuration of network apparatuses in the user home network shown in Fig. 1,
Fig. 26 is a functional block diagram of a SAM in the user home network shown in Fig. 1 and a view of the flow of the data until the secure container received from the content provider is decrypted,
Fig. 27 is a view for explaining data stored in an external memory shown in Fig. 25,
Fig. 28 is a view for explaining data stored in a stack memory,
Fig. 29 is another view of the configuration of the network apparatus in the user home network shown in Fig. 1,
Fig. 30 is a view for explaining data stored in a storage unit shown in Fig. 26,
Fig. 31 is a functional block diagram of the SAM in the user home network shown in Fig. 1 and a view of the flow of the data related to processing for using and/or purchasing the content data,
Fig. 32 is a view for explaining the flow of processing in a transferring side SAM in a case where the content file which is downloaded on a download memory of the network apparatus shown in Fig. 25 and with a purchase form already determined therefor is transferred to the SAM of an AV apparatus,
Fig. 33 is a view of the flow of the data in the transferring side SAM in the case shown in Fig. 32,
Figs. 34A to 34D are views for explaining the format of the secure container for which the purchase form is determined,
Fig. 35 is a view of the flow of the data when writing the input content file etc. in a RAM type or ROM type storage medium in the transferring side SAM in the case shown in Fig. 32,
Fig. 36 is a view for explaining the flow of processing when determining the purchase form in an AV apparatus in a case where the user home network is receives the ROM type storage medium shown in Fig. 7 for which the purchase form of the content has not been determined off-line,
Fig. 37 is a view of the flow of the data in the SAM in the case shown in Fig. 36,
Fig. 38 is a view for explaining the flow of processing when reading the secure container from the ROM type storage medium with the purchase form not yet determined in the AV apparatus in the user home network, transferring this to another AV apparatus, and writing the same in a RAM type storage medium,
Fig. 39 is a view of the flow of the data in the transferring side SAM in the case shown in Fig. 38,
Figs. 40A to 40C are views for explaining the format of the secure container transferred from the transferring side SAM to a transferred side SAM in Fig. 38,
Fig. 41 is a view of the flow of data in the transferred side SAM in the case shown in Fig. 38,
Figs. 42A to 42F are views for explaining the format of the data transmitted and received among the content provider shown in Fig. 1, EMD service center, and SAM by an In-band method, and an out-of-band method,
Figs. 43G to 43J are views for explaining the format of the data transmitted and received among the

content provider shown in Fig. 1, EMD service center, and SAM by the in-band method and the out-of-band method,

Fig. 44 is a view for explaining an example of a connection configuration of apparatuses to buses in the user home network,

Fig. 45 is a view for explaining the data format of a SAM registration list produced by a SAM,

Fig. 46 is a view for explaining the data format of the SAM registration list produced by the EMD service center,

Fig. 47 is a flowchart of the overall operation of the content provider shown in Fig. 1,

Fig. 48 is a view for explaining an example of a delivery protocol of the secure container used in the EMD system of a first embodiment,

Fig. 49 is a view for explaining a second modification of the first embodiment of the present invention,

Fig. 50 is a view for explaining a third modification of the first embodiment of the present invention,

Fig. 51 is a view for explaining a case where a first procedure is employed in a fourth modification of the first embodiment of the present invention,

Fig. 52 is a view for explaining a case where a second procedure is employed in a fourth modification of the first embodiment of the present invention,

Fig. 53 is a view for explaining a fifth modification of the first embodiment of the present invention,

Fig. 54 is a view for explaining a first pattern of a sixth modification of the first embodiment of the present invention,

Fig. 55 is a view for explaining a second pattern of a sixth modification of the first embodiment of the present invention,

Fig. 56 is a view for explaining a third pattern of a sixth modification of the first embodiment of the present invention,

Fig. 57 is a view for explaining a fourth pattern of a sixth modification of the first embodiment of the present invention,

Fig. 58 is a view for explaining a fifth pattern of a sixth modification of the first embodiment of the present invention,

Fig. 59 is an overall view of the configuration of the EMD system of a second embodiment of the present invention,

Fig. 60 is a functional block diagram of the content provider shown in Fig. 59 and a view of the flow of the data related to the secure container transmitted to a service provider,

Fig. 61 is a flowchart showing a routine of processing for delivery of the secure container performed in the content provider,

Fig. 62 is a flowchart showing a routine of the processing for delivery of the secure container performed in the content provider,

Fig. 63 is a functional block diagram of the service provider shown in Fig. 59 and a view of the flow of the data transmitted and received with the user home network,

Fig. 64 is a flowchart showing a routine of the processing for preparation of the secure container performed in the service provider,

Figs. 65A to 65D are views for explaining the format of the secure container transmitted from the service provider shown in Fig. 59 to the user home network,

Fig. 66 is a view for explaining a transmission format of the content file stored in the secure container shown in Fig. 65,

Fig. 67 is a view for explaining the transmission format of the key file stored in the secure container shown in Fig. 65,

Fig. 68 is a functional block diagram of the service provider shown in Fig. 59 and a view of the flow of the data transmitted and received with the EMD service center,

Fig. 69 is a view for explaining the format of a price tag registration request use module transmitted from the service provider to the EMD service center,

Fig. 70 is a functional block diagram of the EMD service center shown in Fig. 59 and a view of the flow of the data related to the data transmitted and received with the service provider,

Fig. 71 is a functional block diagram of the EMD service center shown in Fig. 59 and a view of the flow of the data related to the data transmitted and received with the content provider,

Fig. 72 is a functional block diagram of the EMD service center shown in Fig. 59 and a view of the flow of the data related to the data transmitted and received with the SAM,

Fig. 73 is a view for explaining contents of usage log data,

Fig. 74 is a view of the configuration of the network apparatus shown in Fig. 59,

Fig. 75 is a functional block diagram of a CA module shown in Fig. 74,

Fig. 76 is a functional block diagram of the SAM shown in Fig. 74 and a view of the flow of the data from the input of the secure container to decryption,

Fig. 77 is a view for explaining the data stored in the storage unit shown in Fig. 76,

Fig. 78 is a functional block diagram of the SAM shown in Fig. 74 and a view of the flow of the data in a case where a purchase and/or usage form of the content etc. are determined,

Fig. 79 is a flowchart showing a routine of processing for determining the purchase form of the secure container in the SAM,

Fig. 80 is a view for explaining the format of the key file after the purchase form is determined,

Figs. 81A to 81E are views for explaining the flow of the processing in the transferred side SAM in a case where the content file downloaded on the download memory of the network apparatus shown in Fig. 74 and with the purchase form already de-

termined therefor is transferred to the SAM of the AV apparatus,

Fig. 82 is a view of the flow of the data in the transferring side SAM in the case shown in Fig. 81,

Fig. 83 is a view of the flow of the data in the transferred side SAM in the case shown in Fig. 81,

Fig. 84 is a flowchart of the overall operation of the EMD system shown in Fig. 59,

Fig. 85 is a flowchart of the overall operation of the EMD system shown in Fig. 59,

Fig. 86 is a view for explaining an example of the delivery format of the secure container from the service provider to the user home network in the EMD system of the second embodiment,

Fig. 87 is a view for explaining an example of the delivery protocol of the secure container employed by the EMD system of the second embodiment,

Fig. 88 is a view for explaining the delivery protocol used when delivering the secure container etc. from the user home network to a service provider 310 in Fig. 87,

Fig. 89 is a view for explaining the delivery protocol used when delivering the key file etc. from the content provider to the EMD service center in Fig. 87,

Fig. 90 is a view for explaining the delivery protocol used when delivering a price tag data 312 etc. from the service provider to the EMD service center in Fig. 87,

Fig. 91 is a view for explaining the delivery protocol used when delivering the secure container etc. in the user home network in Fig. 87,

Fig. 92 is a view for explaining an implement format of the secure container to a protocol layer in a case where XML/SMIL/BML is utilized for a data broadcast method of a digital broadcast,

Fig. 93 is a view for explaining the implement format of the secure container to the protocol layer in a case where MHEG is utilized for the data broadcast method of the digital broadcast,

Fig. 94 is a view for explaining the implement format of the secure container to the protocol layer in a case where XML/SMIL is utilized for the data broadcast method of an interface,

Fig. 95 is a view for explaining the delivery protocol used when delivering the usage log data etc. from the user home network to the EMD service center,

Fig. 96 is a view for explaining the delivery protocol used when delivering the secure container etc. in the user home network,

Fig. 97 is a view of the configuration of the EMD system using two service providers according to a first modification of the second embodiment of the present invention,

Fig. 98 is a view of the configuration of the EMD system using a plurality of content providers according to a second modification of the second embodiment of the present invention,

Fig. 99 is a view of the configuration of the EMD system according to a third modification of the second embodiment of the present invention,

Fig. 100 is a view of the configuration of the EMD system according to a fourth modification of the second embodiment of the present invention,

Fig. 101 is a view for explaining a form of a route for acquiring certificate data,

Fig. 102 is a view for explaining processing in a case where the certificate data of the content provider is invalidated,

Fig. 103 is a view for explaining processing in a case where the certificate data of the service provider is invalidated,

Fig. 104 is a view for explaining processing in a case where the certificate data of the SAM is invalidated,

Fig. 105 is a view for explaining another processing in the case where the certificate data of the SAM is invalidated,

Fig. 106 is a view for explaining a case where a right management use clearinghouse and an electronic settlement use clearinghouse are provided in the EMD system shown in Fig. 47 in place of the EMD service center,

Fig. 107 is a view of the configuration of the EMD system in a case where the right management use clearinghouse and the electronic settlement use clearinghouse shown in Fig. 106 are provided in a single EMD service center,

Fig. 108 is a view of the configuration of the EMD system in a case where the service provider directly performs settlement at the electronic settlement use clearinghouse,

Fig. 109 is a view of the configuration of the EMD system in a case where the content provider directly performs settlement at the electronic settlement use clearinghouse,

Fig. 110 is a view of the configuration of the EMD system in a case where the content provider is further provided with functions of both of the right management use clearinghouse and the electronic settlement use clearinghouse,

Fig. 111 is a view for explaining the format of the secure container provided from the content provider to the service provider shown in Fig. 47 in an eighth modification of the second embodiment of the present invention,

Fig. 112 is a view for explaining a link relationship by directory structure data between the content file and the key file shown in Fig. 111,

Fig. 113 is a view for explaining another example of the directory structure between the content file and the key file,

Fig. 114 is a view for explaining the format of the secure container provided from the service provider to the SAM shown in Fig. 47 in the eighth modification of the second embodiment of the present invention,

Fig. 115 is a view for explaining a first concept of

the data format of a composite type secure container,

Fig. 116 is a view for explaining a second concept of the data format of the composite type secure container,

Fig. 117 is a view for explaining a case where a first procedure is employed in the EMD system according to the eighth modification of the second embodiment of the present invention,

Fig. 118 is a view for explaining a case where a second procedure is employed in the EMD system according to the eighth modification of the second embodiment of the present invention,

Fig. 119 is a view for explaining a data format in a case where the file format is not employed in the EMD system according to the eighth modification of the second embodiment of the present invention,

Fig. 120 is a view of the configuration of the EMD system according to a 10th modification of the second embodiment of the present invention,

Fig. 121 is a view of the configuration of the EMD system according to a first pattern of an 11th modification of the second embodiment of the present invention,

Fig. 122 is a view of the configuration of the EMD system according to a second pattern of the 11th modification of the second embodiment of the present invention,

Fig. 123 is a view of the configuration of the EMD system according to a third pattern of the 11th modification of the second embodiment of the present invention,

Fig. 124 is a view of the configuration of the EMD system according to a fourth pattern of the 11th modification of the second embodiment of the present invention,

Fig. 125 is a view of the configuration of the EMD system according to a fifth pattern of the 11th modification of the second embodiment of the present invention,

Fig. 126 is a view of the configuration of the EMD system according to a ninth modification of the second embodiment of the present invention,

Fig. 127 is a view for explaining a file inclusion size relationship of the secure container in the second embodiment of the present invention,

Fig. 128 is a view for explaining the EMD system of a third embodiment of the present invention,

Fig. 129 is a functional block diagram of the EMD service center shown in Fig. 128,

Fig. 130 is a view for explaining a modification of the EMD system of the third embodiment of the present invention,

Fig. 131 is a view for explaining the EMD system of a fourth embodiment of the present invention,

Fig. 132 is a view for explaining a modification of the EMD system of the fourth embodiment of the present invention,

Fig. 133 is a view for explaining the EMD system of a fifth embodiment of the present invention,

Fig. 134 is a view for explaining a modification of the EMD system of the fifth embodiment of the present invention,

Fig. 135 is a view for explaining another modification of the EMD system of the fifth embodiment of the present invention,

Fig. 136 is a view for explaining the EMD system of a sixth embodiment of the present invention,

Fig. 137 is a view for explaining a modification of the EMD system of the sixth embodiment of the present invention,

Fig. 138 is a view for explaining another modification of the EMD system of the sixth embodiment of the present invention,

Fig. 139 is a view for explaining the EMD system of a seventh embodiment of the present invention,

Fig. 140 is a view for explaining a modification of the EMD system of the seventh embodiment of the present invention,

Fig. 141 is a view for explaining another modification of the EMD system of the seventh embodiment of the present invention,

Fig. 142 is a view for explaining the EMD system of an eighth embodiment of the present invention,

Fig. 143 is a view for explaining the EMD system of a ninth embodiment of the present invention,

Fig. 144 is a view for explaining the format of the key file in a case where the key file is produced in the content provider, and

Fig. 145 is a view of the configuration of a conventional EMD system.

BEST MODE FOR WORKING THE INVENTION

[0277] Below, an explanation will be given of an EMD (electronic music distribution) system according to the present embodiment.

First embodiment

[0278] Figure 1 is a view of the configuration of an EMD system 100 of the present embodiment.

[0279] In the present embodiment, the content data distributed to the user means digital. data with the information per se having value and includes image data, audio data, programs (software), etc., but an explanation will be given below by taking as an example music data.

[0280] As shown in Fig. 1, the EMD system 100 has a content provider 101, an EMD service center (clearinghouse, hereinafter, also described as an "ESC") 102, and a user home network 103.

[0281] Here, the content provider 101, EMD service center 102, and SAMs 105_1 to 105_4 correspond to the data providing apparatus, management device, and the data processing apparatuses according to claim 1, claim

6, claim 104, and claim 109.

[0282] First, a brief explanation will be given of the EMD system 100.

[0283] In the EMD system 100, the content provider 101 sends the content key data Kc used when encrypting the content data C of the content to be provided by itself, usage control policy (UCP, certificate of title) data 106 indicating the content of rights such as usage permission conditions of the content data C, and electronic watermark information management data indicating the content and buried location of the electronic watermark information to the EMD service center 102 serving as the reputable authority manager.

[0284] The EMD service center 102 registers (certifies or authorizes) the content key data Kc, usage control policy data 106, and the electronic watermark information key data received from the content provider 101.

[0285] Also, the EMD service center 102 produces a key file KF with the content key data Kc encrypted by the distribution use key data KD_1 to KD_6 of a corresponding period, the usage control policy data 106, and its own signature data stored therein and sends this to the content provider 101.

[0286] Here, the signature data is used for verifying existence of tampering with the key file KF, the legitimacy of the author of the key file KF, and the fact that the key file KF was normally registered in the EMD service center 102.

[0287] Also, the content provider 101 encrypts the content data C by the content key data Kc and distributes a secure container (module of the present invention) 104 storing the related produced content file CF, key file KF received from the EMD service center 102, its own signature data, etc. therein to the user home network 103 by using a network such as the Internet, digital broadcast, or package media such as storage media.

[0288] Here, the signature data stored in the secure container 104 is used for verifying the existence of tampering with the corresponding data and the legitimacy of the author and transmitter of the related data.

[0289] The user home network 103 has for example a network apparatus 160_1 and AV apparatuses 160_2 to 160_4.

[0290] The network apparatus 160_1 includes a built-in SAM (secure application module) 105_1.

[0291] The AV apparatuses 160_2 to 160_4 include built-in SAMs 105_1 to 105_4. The SAMs 105_1 to 105_4 are connected to each other via a bus 191 for example an IEEE (Institute of Electrical and Electronics Engineers) 1394 serial interface bus.

[0292] The SAMs 105_1 to 105_4 decrypt the secure container 104 received by the network apparatus 160_1 via the network or the like from the content provider 101 on-line and/or the secure container 104 received at the AV apparatuses 160_2 to 160_4 from the content provider 101 via storage media off-line by using the distribution use key data KD_1 to KD_3 of the corresponding period, then perform the verification of the signature data.

[0293] The secure container 104 supplied to the SAMs 105_1 to 105_4 becomes the object of the reproduction, recording to a storage medium etc. after the purchase and/or usage form is determined by an operation of the users in the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4.

[0294] The SAMs 105_1 to 105_4 record the log of the purchase and/or usage form of the secure container 104 as usage log data 108 and, at the same time, produce usage control status data 166 indicating the purchase form.

[0295] The usage log data 108 is transmitted from the user home network 103 to the EMD service center 102 in response to for example a request from the EMD service center 102.

[0296] The usage control status data 166 is transmitted from the user home network 103 to the EMD service center 102 whenever for example the purchase form is determined.

[0297] The EMD service center 102 determines (calculates) a charge content based on the usage log data 108 and performs settlement at a settlement manager 91 such as a bank via a payment gateway 90. By this, the money paid to the settlement manager 91 by the user of the user home network 103 is paid to the content provider 101 by the settlement processing by the EMD service center 102.

[0298] Also, the EMD service center 102 transmits the settlement report data 107 to the content provider 101 at every predetermined period.

[0299] In the present embodiment, the EMD service center 102 has a certificate authority function, a key data management function, and a right clearing (profit distribution) function.

[0300] Namely, the EMD service center 102 functions as a second certificate authority with respect to a route certificate authority 92 as the highest authority manager located at a neutral position (located in the lower layer of the route certificate authority 92) and certifies the legitimacy of the related public key data by attaching a signature by secret key data of the EMD service center 102 to the certificate data of the public key data used for the verification processing of the signature data in the content provider 101 and SAMs 105_1 to 105_4. Also, as mentioned above, the registration and authorization of the usage control policy data 106 of the content provider 101 by the EMD service center 102 is one of the certificate authority functions of the EMD service center 102.

[0301] Also, the EMD service center 102 has a key data management function for managing the key data, for example, the distribution use key data KD_1 to KD_6.

[0302] Also, the EMD service center 102 has a right clearing (profit distribution) function of performing settlement for a purchase and/or usage of the content by the user based on the suggested retailer' price SRP described in the authorized usage control policy data 106 and the usage log data 108 input from the SAMs 105_1

to 105_4 and distributing money paid by the user to the content provider 101.

[0303] Figure 2 is a view summarizing the concept of the secure container 104.

[0304] As shown in Fig. 2, in the secure container 104, the content file CF produced by the content provider 101 and the key file KF produced by the EMD service center 102 are stored.

[0305] In the content file CF, header data containing the header portion and the content ID, the encrypted content data C using the content key data Kc, and the signature data using a secret key data $K_{CP,S}$ of the content provider 101 for them are stored.

[0306] In the key file KF, the header data containing the header portion and the content ID, the content key data Kc, and the usage control policy data 106 encrypted by the distribution use key data KD_1 to KD_6 and the signature data by secret key data $K_{ESC,S}$ of the EMD service center 102 for them are stored.

[0307] Below, a detailed explanation will be given of the components of the content provider 101.

[Content Provider 101]

[0308] Figure 3 is a functional block diagram of the content provider 101 and shows the flow of the data related to the data transmitted and received with the SAMs 105_1 to 105_4 of the user home network 103.

[0309] Also, in Fig. 4, the flow of the data related to the data transmitted and received between the content provider 101 and the EMD service center 102 is shown.

[0310] Note that, in Fig. 4 and the following drawings, the flow of the data input and output to and from the signature data processing unit and the encryption and/or decryption unit using session key data K_{SES} is omitted.

[0311] As shown in Fig. 3 and Fig. 4, the content provider 101 has a content master source database 111, an electronic watermark information addition unit 112, a compression unit 113, an encryption unit 114, a random number generation unit 115, an expansion unit 116, a signature processing unit 117, a secure container preparation unit 118, a secure container database 118a, a key file database 118b, a storage unit (database) 119, a mutual certification unit 120, an encryption and/or decryption unit 121, a usage control policy data preparation unit 122, an audial check unit 123, a SAM management unit 124, an EMD service center management unit 125, and a content ID generation unit 850.

[0312] The content provider 101 registers for example its own generated public key data, ID, and its own bank account number (account number for settlement) in the EMD service center 102 off-line before communicating with the EMD service center 102 and acquires its own identifier (identification number) CP_ID. Also, the content provider 101 receives the public key data of the EMD service center 102 and the public key data of the route certificate authority 92 from the EMD service center 102.

[0313] Below, an explanation will be given of the functional blocks of the content provider 101 shown in Fig. 3 and Fig. 4.

[0314] The content master source database 111 stores the content data as the master source of the content to be provided to the user home network 103 and outputs content data S111 to be provided to the electronic watermark information addition unit 112.

[0315] The electronic watermark information addition unit 112 buries a source watermark Ws, a copy control watermark Wc, a user watermark Wu, a link watermark WL, etc. in the content data S111 to produce content data S112 and outputs the content data S112 to the compression unit 113.

[0316] The source watermark Ws is information concerning the copyright such as the name of the copyright owner of the content data, the ISRC code, authoring date, authoring apparatus ID (identification data), and destination of distribution of the content.

[0317] The copy control watermark Wc is information containing a copy prohibition bit for prevention of copying via an analog interface.

[0318] The user watermark Wu contains, for example, the identifier CP_ID of the content provider 101 for specifying the origin of distribution and the destination of distribution of the secure container 104 and identifiers SAM_ID_1 to SAM_ID_4 of the SAMs 105_1 to 105_4 of the user home network 103.

[0319] The link watermark WL contains for example the content ID of the content data C.

[0320] By burying the link watermark WL in the content data C, even in a case where the content data C is distributed by an analog broadcast for example a television or AM/FM radio, the EMD service center 102 can introduce a content provider 101 handling the related content data C to the user in response to a request from the user. Namely, by detecting the link watermark WL buried in the content data C utilizing an electronic watermark information decoder at the receiving location of the related content data C and transmitting the content ID contained in the related detected link watermark WL to the EMD service center 102, the EMD service center 102 can introduce the content provider 101 etc. handling the related content data C to the related user.

[0321] Concretely, for example, if the user pushes a predetermined button at a point of time when he thinks that the music being broadcast is good while listening to the radio in a car, the electronic watermark information decoder built-in the related radio detects the content ID contained in the link watermark WL buried in the related content data C, a communication address, etc. of the EMD service center 102 registering the related content data C etc., and stores the related detected data in a media SAM carried in for example a memory stick or other semiconductor memory or an MD (Mini Disc) or other optical disc or other portable medium. Then, he sets the related movable media in the network appara-

tus carrying a SAM connected to the network. Then, after mutual certification by the related SAM and the EMD service center 102, he transmits the personal information carried in the media SAM and the stored content ID etc. from the network apparatus to the EMD service center 102. Thereafter, the network apparatus receives an introduction list etc. of the content provider 101 etc. handling the related content data C from the EMD service center 102.

[0322] In addition, for example, when the EMD service center 102 receives the content ID etc. from the user, the information specifying the related user may be notified to the content provider 101 providing the content data C corresponding to the related content ID. In this case, the content provider 101 receiving the related communication transmits the related content data C to the network apparatus of the user if the related user is a contracting subscriber or may transmit promotional information concerning itself to the network apparatus of the user if the related user is not a contracting subscriber.

[0323] Note that, in the second embodiment mentioned later, an EMD service center 302 can introduce a service provider 310 handling the related content data C to the user based on the link watermark WL.

[0324] Also, in the present embodiment, preferably, the content and buried location of each electronic watermark information are defined as a watermark module WM, and the watermark module WM is registered and managed in the EMD service center 102. The watermark module WM is used when for example the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4 in the user home network 103 verify the legitimacy of the electronic watermark information.

[0325] For example, in the user home network 103, by deciding that the electronic watermark information is legitimate where both of the buried location of the electronic watermark information and the content of the buried electronic watermark information match based on the user watermark module managed by the EMD service center 102, the burial of a false electronic watermark information can be detected with a high probability.

[0326] The compression unit 113 compresses the content data S112 by an acoustic compression method, for example ATRAC3 (Adaptive Transform Acoustic Coding 3) (trademark), and outputs compressed content data S113 to the encryption unit 114.

[0327] In this case, at the time of compression by the compression unit 113, it is also possible to bury the electronic watermark information in the content data again. Concretely, as shown in Fig. 3, when the content data 113 is expanded at the expansion unit 116 to produce content data S116 and the content data S116 is reproduced at the audial check unit 123, the influence exerted upon the quality of sound by the burial of the electronic watermark information is decided by for example a person actually listening to it. Where it does not satisfy a predetermined standard, the electronic watermark information addition unit 112 is instructed to perform the processing for burying the electronic watermark information again.

[0328] By this, when employing an acoustic compression method accompanied by for example loss of data, it is possible to adequately cope with the case where the buried electronic watermark information is lost due to the related compression. Further, it is also possible to expand the compressed content data again and confirm whether or not the buried electronic watermark information can be correctly detected. In this case, the feeling of the sound quality is also verified. Where there is a problem in the sound, the burial of the electronic watermark information is adjusted. For example, where the electronic watermark information is buried by using a masking effect, the layer for burying the electronic watermark information is adjusted.

[0329] The encryption unit 114 uses the content key data Kc as the common key, encrypts the content data S113 by a common key encryption method such as DES (Data Encryption Standard) or Triple DES to produce the content data C, and outputs this to the secure container preparation unit 118.

[0330] Also, the encryption unit 114 encrypts an A/V expansion use software Soft, a meta data Meta, and the watermark module WM by using the content key data Kc as the common key and then outputs them to the secure container preparation unit 117.

[0331] DES is the encryption method for processing 64 bits of plain text as one block by using a common key of 56 bits. The processing of DES is comprised of a portion for scrambling the plain text to convert the same to encrypted text (data scrambling portion) and a portion for creating the key (magnification key) data used in the data scrambling portion from the common key data (key processing portion). All algorithms of the DES are public, therefore, here, the basic processing of the data scrambling portion will be simply explained.

[0332] First, 64 bits of the plain text are divided to H_0 of the upper significant 32 bits and L_0 of lower significant 32 bits. By receiving as input the magnification key data K_1 of 48 bits supplied from the key processing unit and the L_0 of the lower significant 32 bits, the output of an F function scrambled L_0 of the lower significant 32 bits is calculated. The F function is comprised of two types of basic transforms of "substitution" of switching numerical values by a predetermined rule and "transposition" of switching bit locations by a predetermined rule. Next, an exclusive OR of the H_0 of the upper significant 32 bits and the output of the F function is calculated, and the result thereof is defined as L_1. Also, L_0 is made H_1.

[0333] Then, based on the H_0 of the upper significant 32 bits and the L_0 of the lower significant 32 bits, the above processing is repeated 16 times. The obtained H_{16} of the upper significant 32 bits and L_{16} of the lower significant 32 bits are output as the encrypted text. The decryption is realized by inversely following the sequence by using the common key data used for the en-

cryption.

[0334] The random number generation unit 115 generates a random number of a predetermined number of bits and stores the related random number as the content key data Kc in the storage unit 119.

[0335] Note that, it is also possible if the content key data Kc is produced from the information concerning a song provided by the content data. The content key data Kc is updated for example every predetermined time.

[0336] Also, where a plurality of content providers 101 exist, it is also possible to use inherent content key data Kc from individual content providers 101 or it is also possible to use the content key data Kc common to all content providers 101.

[0337] In the key file database 118b, as shown in Fig. 4, the key file KF shown in Fig. 5B received from the EMD service center 102 via the EMD service center management unit 125 is stored. The key file KF exists for every content data C. As will be mentioned later, a link is designated with the corresponding content file CF by directory structure data DSD in the header of the content file CF.

[0338] In the key file KF, as shown in Fig. 5B and Fig. 7, the header, content key data Kc, usage control policy data 106 (usage permission condition) 106, SAM program download containers SDC_1 to SDC_3, and signature data $SIG_{K1,ESC}$ are stored.

[0339] Here, as the signature data using the secret key data $K_{ESC,S}$ of the content provider 101, use can be also made of the signature data $K_{1,ESC}$ for all data stored in the key file KF as shown in Fig. 5B. Alternatively, signature data for the data from the header to the information concerning the key file, signature data for the content key data Kc and the usage control policy data 106, and signature data for the SAM program download container SDC can be separately provided too as shown in Fig. 7.

[0340] The content key data Kc and usage control policy data 106 and the SAM program download containers SDC_1 to SDC_3 are encrypted by using the distribution use key data KD_1 to KD_6 of the corresponding periods.

[0341] In the header data, as shown in Fig. 7, a synchronization signal, the content ID, the signature data by the secret key data $K_{ESC,S}$ of the content provider 101 for the content ID, the directory structure data, hyper link data, the information concerning the key file KF, the signature data by the secret key data $K_{ESC,S}$ of the content provider 101 for the directory structure data, etc. are contained.

[0342] Note that, as the information to be contained in the header data, various information can be considered and freely varied according to the situation. For example, it is also possible if the information as shown in Fig. 8 is contained in the header data.

[0343] Also, in the content ID, for example, the information as shown in Fig. 9 is contained. The content ID is produced in the EMD service center 102 or the content provider 101. Where it is produced in the EMD service center 102, the signature data by the secret key data $K_{ESC,S}$ of the EMD service center 102 is added as shown in Fig. 9, while where it is produced at the content provider 101, the secret key data $K_{CP,S}$ of the content provider 101 is added.

[0344] The content ID is produced by for example the content ID generation unit 850 as shown in Fig. 4 and stored in the storage unit 119. Note that, it is also possible if the content ID is produced by the EMD service center 102.

[0345] The directory structure data indicates correspondence among the content files CF in the secure container 104 and correspondence between the content files CF and the key files KF.

[0346] For example, where the content files CF_1 to CF_3 and the key files KF_1 to KF_3 corresponding to them are stored in the secure container 104, as shown in Fig. 10, the links among the content files CF_1 to CF_3 and the links between the content files CF_1 to CF_3 and the key files KF_1 to KF_3 are established by the directory structure data.

[0347] The hyper link data indicates a hierarchy structure among the key files KF and the correspondence between the content files CF and the key files KF covering all files inside and outside the secure container 104.

[0348] Concretely, as shown in Fig. 11, the address information of the linked site for every content file CF and key file KF and the certificate value (hash value) thereof are stored in the secure container 104. The links are verified by comparing the hash value of one's own address information obtained by using the hash function H(x) and the certificate value of the other party.

[0349] Also, in the usage control policy data 106, as shown in Fig. 7, the content ID, identifier CP_ID of the content provider 101, an expiration date of the usage control policy data 106, the communication address of the EMD service center 102, usage space examination information, wholesale price information, a handling plan, handling control information, handling control information of a commodity demo, the signature data for them, etc. are contained.

[0350] Note that, as in the second embodiment mentioned later, where a secure container 304 is transmitted via the service provider 310 to a user home network 303, in the usage control policy data 106, an identifier SP_ID of the service provider 310 for providing the secure container 104 by the content provider 301 is contained.

[0351] Also, in the SAM program download containers SDC_1 to SDC_3, as shown in Fig. 7, a download driver indicating the routine of the download used when downloading a program in the SAMs 105_1 to 105_4, a label reader such as an UCP-L (Label) R (Reader) indicating a syntax (grammar) of the usage control policy data (UCP) U106, lock key data for locking/unlocking rewriting and erasing of the storage units (flash-ROM) built in the SAMs 105_1 to 105_4 in block units, and the signature data for them are contained.

[0352] Note that, the storage unit 119 is provided with

various databases including for example a database for storing the certificate data.

[0353] The signature processing unit 117 obtains the hash value of the data covered by the signature and produces the signature data SIG thereof by using the secret key data $K_{CP,S}$ of the content provider 101.

[0354] Note that, the hash value is produced by using a hash function. A hash function is a function receiving as input the data covered, compressing the related input data to data having a predetermined bit length, and outputting the same as the hash value. The hash function has as its characteristic feature that it is difficult to predict the input of the hash function from the hash value (output). When one bit input to the hash function varies, many bits of the hash value vary, so it is difficult to find the input data having an identical hash value.

[0355] The secure container preparation unit 118 produces the content file CF storing the header data, meta data Meta, the content data C, A/V expansion use software Soft, and the watermark module WM input from the encryption unit 114 and encrypted by the content key data Kc therein as shown in Fig. 5A.

[0356] It is also possible to contain the file reader and the signature data of the file reader in the secret key data $K_{CP,S}$ as shown in Fig. 6. By doing this, in the SAMs 105_1 to 105_4, a plurality of secure containers 104 storing the content files CF of different formats received from a plurality of secure containers 104 of different streams can be efficiently processed.

[0357] Here, the file reader is used when reading a content file CF and the key file KF corresponding to that and indicates the reading routine etc. of these files.

[0358] Note, in the present embodiment, a case where the related file reader is transmitted in advance from the EMD service center 102 to the SAMs 105_1 to 105_4 is exemplified. Namely, in the present embodiment, the content file CF of the secure container 104 does not store the file reader.

[0359] In the header data, as shown in Fig. 6, the synchronization signal, content ID, signature data by the secret key data $K_{CP,S}$ of the content provider 101 for the content ID, directory information, hyper link information, serial number, expiration date and producer information of the content file CF, file size, existence of encryption, encryption algorithm, information concerning the signature algorithm, signature data by the secret key data $K_{CP,S}$ of the content provider 101 concerning the directory information, etc. are contained.

[0360] In the meta data Meta, as shown in Fig. 6, explanatory text of the commodity (content data C), commodity demo and PR information, information related to the commodity, and the signature data from the content provider 101 for them are contained.

[0361] In the present invention, as shown in Fig. 5 and Fig. 6, the case where the meta data Meta is stored in the content file CF and transmitted is exemplified, but it is also possible not to store the meta data Meta in the content file CF, but transmit the same from the content provider 101 to the SAM 105_1 etc. through a route different from the route for transmitting the content file CF.

[0362] The A/V expansion use software Soft is the software used when expanding the content file CF in the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4 of the user home network 103 and is the expansion use software of for example the ATRAC3 method.

[0363] In this way, by storing the A/V expansion use software Soft in the secure container 104, the content data C can be expanded by using the A/V expansion use software Soft stored in the secure container 104 in the SAMs 105_1 to 105_4. Even if the compression and expansion method of the content data C is freely set by the content provider 101 for every content data C or every content provider 101, a large load will not be imposed on the user.

[0364] The watermark module WM contains for example the information required for detecting the electronic watermark information buried in the content data C and software as mentioned before.

[0365] Also, the secure container preparation unit 118 produces the secure container 104 storing the content file CF shown Fig. 5A mentioned above, signature data $SIG_{6,CP}$ of the related content file CF, the key file KF shown in Fig. 5B corresponding to the related content file CF read out from the key file database 118b, signature data $SIG_{7,CP}$ of the related key file KF, certificate data CER_{CP} of the content provider 101 read out from the storage unit 119, and signature data $SIG_{1,ESC}$ of the related certificate data CER_{CP} therein.

[0366] Here, the signature data $SIG_{6,CP}$ is used for verifying the legitimacy of the producer and transmitter of the content file CF at the received site of the secure container 104.

[0367] Here, the signature data $SIG_{7,CP}$ is used for verifying the legitimacy of the transmitter of the key file KF at the received site of the secure container 104. Note that, at the received site of the secure container 104, the legitimacy of the producer of the key file KF is verified based on the signature data $SIG_{K1,ESC}$ in the key file KF. Also, the signature data $SIG_{K1,ESC}$ is used also for verifying whether or not the key file KF is registered in the EMD service center 102.

[0368] In the present embodiment, the encrypted content data C is stored in the secure container 104 in a form not depending upon the compression method of the content data C, existence of compression, encryption method (including both the cases of the common key encryption method and public key encryption method), parameters of the signals giving the content data C (sampling frequency etc.), and the preparation method (algorithm) of the signature data. Namely, these items can be freely determined by the content provider 101.

[0369] Also, the secure container preparation unit 118 outputs the secure container 104 stored in the secure container database 118a to the SAM management unit 124 in response to a request from the user.

[0370] In this way, in the present embodiment, an in-

band method of storing the certificate CER_{CP} of the public key data $K_{CP,P}$ of the content provider 101 in the secure container 104 and transmitting the same to the user home network 103 is employed. Accordingly, the user home network 103 does not have to communicate with the EMD service center 102 for obtaining the certificate CER_{CP}.

[0371] Note that, in the present invention, it is also possible to employ an out-of-band method of obtaining the certificate CER_{CP} from the EMD service center 102 by the user home network 103 without storing the certificate CER_{CP} in the secure container 104.

[0372] The mutual certification unit 120 performs mutual certification between the EMD service center 102 and the user home network 103 to produce the session key data (common key) K_{SES} when the content provider 101 transmits or receives data on-line with the EMD service center 102 and the user home network 103. The session key data K_{SES} is newly produced at each mutual certification.

[0373] The encryption and/or decryption unit 121 encrypts the data to be transmitted on-line to the EMD service center 102 and the user home network 103 by the content provider 101 by using the session key data K_{SES}.

[0374] Also, the encryption and/or decryption unit 121 decrypts the data received on-line from the EMD service center 102 and the user home network 103 by the content provider 101 by using the session key data K_{SES}.

[0375] The usage control policy data preparation unit 122 produces the usage control policy data 106 and outputs this to the EMD service center management unit 125.

[0376] The usage control policy data 106 is a descriptor defining operating rules of the content data C and for example describes the suggested retailer's price SRP intended by an operator of the content provider 101, copy rule of the content data C, etc.

[0377] The SAM management unit 124 supplies the secure container 104 off-line or on-line to the user home network 103.

[0378] Also, when distributing the secure container 104 to the SAMs 105_1 to 105_4 on-line, the SAM management unit 124 uses, as the communication protocol for transmitting the secure container 104, an MHEG (Multimedia and Hypermedia Information Coding Experts Group) protocol if a digital broadcast or uses an XML/SMIL/HTML (Hyper TextMarkup Language) if the Internet and buries the secure containers 104 in these communication protocols in a form not depending upon the coding method by tunneling.

[0379] Accordingly, it is not necessary to match formats between the communication protocol and the secure container 104, so the format of the secure container 104 can be flexibly set.

[0380] Note that, the communication protocol used when transmitting the secure container 104 from the content provider 101 to the user home network 103 is not limited to those mentioned above and may be any protocol.

[0381] Figure 12 is a view for explaining a storage medium 130_1 of a ROM type used in the present embodiment.

[0382] As shown in Fig. 12, the ROM type storage medium 130_1 has a ROM region 131, a secure RAM region 132, and a media SAM 133.

[0383] In the ROM region 131, the content file CF shown in Fig. 5A is stored.

[0384] Also, the secure RAM region 132 is a region where predetermined permission (certification) is necessary for accessing the stored data. Signature data produced by using a MAC (Message Authentication Code) function with the key file KF and the certificate data CER_{CP} and a storage use key data K_{STR} having an inherent value in accordance with the type of the apparatus shown in Figs. 5B and 5C as factors and the data obtained by encrypting the related key file KF and the certificate data CER_{CP} by using media key data K_{MED} having an inherent value in the storage medium are stored.

[0385] Also, in the secure RAM region 132, for example, certificate revocation data (revocation list) for specifying the content provider 101 and the SAMs 105_1 to 105_5 which became invalid due to illegitimate actions or the like is stored.

[0386] Also, in the secure RAM region 132, as will be mentioned later, usage control status (UCS) data 166 etc. produced when the purchase and/or usage form of the content data C is determined in the SAMs 105_1 to 105_4 of the user home network 103 is determined are stored. By this, by the storage of the user control status data 166 in the secure RAM region 132, a ROM type storage medium 130 with a purchase and/or usage form determined therein is obtained.

[0387] In the media SAM 133, for example the media ID serving as the identifier of the ROM type storage medium 130_1 and the media key data K_{MED} are stored.

[0388] The media SAM 133 has for example a mutual certificate authority function.

[0389] As the storage medium of the ROM type used in the present embodiment, for example, other than one shown in Fig. 12, also a ROM type storage medium 130_2 shown in Fig. 13 and a ROM type storage medium 130_3 shown in Fig. 14 can be considered.

[0390] The ROM type storage medium 130_2 shown in Fig. 13 has the ROM region 131 and the media SAM 133 having the certificate authority function, but is not provided with the secure RAM region 132 as in the ROM type storage medium 130_1 shown in Fig. 12. Where use is made of the ROM type storage medium 130_2, the content file CF is stored in the ROM region 131, and the key file KF is stored in the media SAM 133.

[0391] Also, the ROM type storage medium 130_3 shown in Fig. 14 has the ROM region 131 and the secure RAM region 132 and does not have the media SAM 133 as in the ROM type storage medium 130_1 shown in Fig.

12. Where the ROM type storage medium 130_3 is used, the content file CF is stored in the ROM region 131, and the key file KF is stored in the secure RAM region 132. Also, where the ROM type storage medium 130_3 is used, mutual certification is not carried out with the SAM.

[0392] Also, in the present embodiment, other than the ROM type storage medium, also a RAM type storage medium is used.

[0393] As the RAM type storage medium used in the present embodiment, there is, for example, as shown in Fig. 15, a RAM type storage medium 130_4 having the media SAM 133, secure RAM region 132, and nonsecure RAM region 134. In the RAM type storage medium 130_4, the media SAM 133 has the certificate authority function and stores the key file KF. Also, in the RAM region 134, the content file CF is stored.

[0394] Also, as the RAM type storage medium used in the present embodiment, other than that, also a RAM type storage medium 130_5 shown in Fig. 16 and a RAM type storage medium 130_6 shown in Fig. 17 can be considered.

[0395] The RAM type storage medium 130_5 shown in Fig. 16 has the nonsecure RAM region 134 and the media SAM 133 having the certificate authority function, but is not provided with the secure RAM region 132 as in the RAM type storage medium 130_4 shown in Fig. 15. Where the RAM type storage medium 130_5 is used, the content file CF is stored in the RAM region 134, and the key file KF is stored in the media SAM 133.

[0396] Also, the RAM type storage medium 130_6 shown in Fig. 17 has the secure RAM region 132 and the nonsecure RAM region 134, but does not have the media SAM 133 as in the RAM type storage medium 130_4 shown in Fig. 15. Where use is made of the RAM type storage medium 130_6, the content file CF is stored in the RAM region 134, and the key file KF is stored in the secure RAM region 132. Also, where use is made of the RAM type storage medium 130_6, mutual certification is not carried out with the SAM.

[0397] Also, where the secure container 104 is distributed on-line to the user home network 103 by using a network or a digital broadcast, the SAM management unit 124 encrypts the secure container 104 by using the session key data K_{SES} in the encryption and/or decryption unit 121, and then distributes the same via the network to the user home network 103.

[0398] In the present embodiment, as the SAM management unit and the EMD service center management unit and the content provider management unit and service provider management unit mentioned later, use is made of a communication gateway having a tamper resistant structure whereby for example monitoring and tampering of the processing content of the internal portion cannot be carried out or are difficult.

[0399] Here, in both of the case where the content data C is distributed from the content provider 101 to the user home network 103 by using the storage medium 130_1 and the case where it is distributed on-line by using the network, use is made of the secure container 104 of a common form with the usage control policy data 106 stored therein. Accordingly, in the SAMs 105_1 to 105_4 of the user home network 103, the rights clearing based on the common usage control policy data 106 can be carried out in both of the cases of off-line and on-line.

[0400] Also, as mentioned above, in the present embodiment, the in-band method of enclosing the content data C encrypted by the content key data Kc and the content key data Kc for decrypting the related encryption in the secure container 104 is employed. In the in-band method, when it is intended to reproduce the content data C by the apparatus of the user home network 103, it is not necessary to separately distribute the content key data Kc, so there is an advantage that the load of the network communication can be reduced. Also, the content key data Kc has been encrypted by the distribution use key data KD_1 to KD_6, but the distribution use key data KD_1 to KD_6 are managed at the EMD service center 102 and distributed to the SAMs 105_1 to 105_5 of the user home network 103 in advance (when the SAMs 105_1 to 105_4 access the EMD service center 102 for the first time), therefore, in the user home network 103, the usage of the content data C off-line becomes possible without connecting with the EMD service center 102 on-line.

[0401] Note that, the present invention has the flexibility to employ the out-of-band method for separately supplying the content data C and the content key data Kc to the user home network 103 as will be mentioned later.

[0402] When receiving the settlement report data 107 from the EMD service center 102, the EMD service center management unit 125 decrypts it at the encryption and/or decryption unit 121 by using the session key data K_{SES} and then stores the same in the storage unit 119.

[0403] As the settlement report data 107, for example, the content of the settlement concerning the content provider 101 performed by the EMD service center 102 at the settlement manager 91 shown in Fig. 1 is described.

[0404] Also, the EMD service center management unit 125 transmits the content ID as a global unique identifier of the content data C to be provided, a public key data $K_{CP,P}$, and signature data $SIG_{9,CP}$ of them to the EMD service center 102 and receives as input the certificate data CER_{CP} of the public key data $K_{CP,P}$ from the EMD service center 102.

[0405] Also, the EMD service center management unit 125 produces, as shown in Fig. 18, a registration module Mod_2 storing the content ID as the global unique identifier of the content data C to be provided, the content key data Kc, the usage control policy data 106, the watermark module WM, CP_ID as the global unique identifier of the content provider 101, and signature data $SIG_{M1,CP}$ by the secret key data $K_{CP,S}$ of the content provider 101 for them therein when registering the con-

tent key data Kc, the usage control policy data 106, and the watermark module WM in the EMD service center 102 and receiving the key file KF for each of the content data C. Then, the EMD service center 125 encrypts the registration module Mod_2 in the encryption and/or decryption unit 121 by using the session key data K_{SES} and then transmits the same via the network to the EMD service center 102. As the EMD service center management unit 125, as mentioned above, for example use is made of a communication gateway having a high tamper resistant structure whereby monitoring or tampering of the processing content of the internal portion cannot be carried out or are difficult.

[0406] Below, an explanation will be given of the flow of the processing in the content provider 101 by referring to Fig. 3 and Fig. 4.

[0407] Note that, as a prerequisite for performing the following processing, the interested party of the content provider 101 performs the registration processing for the EMD service center 102 off-line by using for example its own ID and a bank account for performing the settlement processing and acquires the global unique identifier CP_ID. The identifier CP_ID is stored in the storage unit 119.

[0408] First, an explanation will be given of the processing where the content provider 101 requests the certificate data CER_{CP} for proving the legitimacy of the public key data $K_{CP,S}$ corresponding to its own secret key data $K_{CP,S}$ from the EMD service center 102 by referring to Fig. 4.

[0409] The content provider 101 generates a random number by using a true random number generator to produce the secret key data $K_{CP,S}$, produces the public key data $K_{CP,P}$ corresponding to the related secret key data $K_{CP,S}$ and stores the same in the storage unit 119.

[0410] The EMD service center management unit 125 reads out the identifier CP_ID and the public key data $K_{CP,P}$ of the content provider 101 from the storage unit 119.

[0411] Then, the EMD service center management unit 125 transmits the identifier CP_ID and the public key data $K_{CP,P}$ to the EMD service center 102.

[0412] Then, the EMD service center management unit 125 receives as input the certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof from the EMD service center 102 in accordance with the related registration and writes them into the storage unit 119.

[0413] Next, an explanation will be given of the processing where the content provider 101 registers the content key data Kc, usage control policy data 106, and the watermark module WM in the EMD service center 102 and receives the key file KF corresponding to the content data C by referring to Fig. 4, Fig. 18, and Fig. 19.

[0414] The registration of the usage control policy data 106 etc. is carried out for individual content data C.

[0415] Figure 19 is a flowchart for explaining the registration processing from the content provider 101 to the EMD service center 102.

[0416] Step A1: Mutual certification is carried out between the mutual certification unit 120 of the content provider 101 shown in Fig. 4 and the EMD service center 102.

[0417] Step A2: The session key data K_{SES} obtained by the mutual certification performed at step A1 is shared by the content provider 101 and the EMD service center 102.

[0418] Step A3: The content provider 101 reads out the content ID, content key data Kc, usage control policy data 106, watermark module WM, and CP_ID, etc. to be registered into the EMD service center 102 from the database of the storage unit 119 etc.

[0419] Step A4: In the signature processing unit 117, the signature data $SIG_{M1,CP}$ indicating the legitimacy of the sender is produced for a module containing for example the usage control policy data 106 read out at step A3 by using the secret key data $K_{CP,S}$ of the content provider 101.

[0420] Then, the EMD service center management unit 125 produces the registration use module Mod_2 storing the content ID, content key data Kc, usage control policy data 106, watermark module WM and CP_ID, and the signature data $SIG_{M1,CP}$ for them therein as shown in Fig. 18.

[0421] Step A5: The encryption and/or decryption unit 121 encrypts the registration use module Mod_2 produced at step A4 by using the session key data K_{SES} shared at step A2.

[0422] Step A6: The EMD service center management unit 125 transmits the registration use module Mod_2 encrypted at step A5 to the EMD service center 102.

[0423] The processing of step A7 and following processing are the processing in the EMD service center 102.

[0424] Step A7: The EMD service center 102 decrypts the received registration use module Mod_2 by using the session key data K_{SES} shared at step A2.

[0425] Step A8: The EMD service center 102 verifies the signature data $SIG_{M1,CP}$ stored in the decrypted registration use module Mod_2 by using the public key data $K_{CP,P}$, confirms the legitimacy of the sender of the registration use module Mod_2, and performs the processing of step A9 under the condition that the legitimacy of the sender is proved.

[0426] Step A9: The EMD service center 102 stores and registers the content ID, content key data Kc, usage control policy data 106, watermark module WM, and CP_ID stored in the registration use module Mod_2 in the predetermined database.

[0427] Note that, the EMD service center management unit 125 receives, as shown in Fig. 18, for example six months' worth of the key files KF from the EMD service center 102 after the registration processing in accordance with the registration use module Mod_2 is carried out for the EMD service center 102, decrypts the related received key files KF by using the session key

data K_{SES} obtained by the mutual certification between the mutual certification unit 120 and the EMD service center 102, and then stores the same in the key file database 118b.

[0428] Next, an explanation will be given of the processing where the content provider 101 transmits the secure container 104 to the SAM 105_1 of the user home network 103 by referring to Fig. 3 and Fig. 4.

[0429] Note that, in the following example, the case where the secure container 104 is transmitted from the content provider 101 to the SAM 105_1 is exemplified, but the case where the secure container 104 is transmitted to each of the SAMs 105_2 to 105_4 is the same except it transmitted to each of the SAMs 105_2 to 105_4 via the SAM 105_1.

[0430] First, as shown in Fig. 3, the content data S111 is read out from the content master source database 111 and output to the electronic watermark information addition unit 112.

[0431] Next, the electronic watermark information addition unit 112 buries the electronic watermark information in the content data S111 to produce the content data S112 and outputs this to the compression unit 113.

[0432] Next, the compression unit 113 compresses the content data S112 by for example the ATRAC3 method to produce the content data S113 and outputs this to the encryption unit 114.

[0433] Also, as shown in Fig. 4, the content key data Kc is produced by generating a random number at the random number generation unit 115, and the related produced content key data Kc is stored in the storage unit 119.

[0434] Next, the encryption unit 114 encrypts the content data S113 input from the compression unit 113, meta data Meta read out from the storage unit 119, the A/V expansion use software Soft and the watermark module WM by using the content key data Kc and outputs the same to the secure container preparation unit 118. In this case, it is also possible if the meta data Meta and the watermark module WM are not encrypted.

[0435] Then, the secure container preparation unit 118 produces,the content file CF shown in Fig. 5A. Also, in the signature processing unit 117, the hash value of the content file CF is obtained and the signature data $SIG_{6,CP}$ is produced by using the secret key data $K_{CP,S}$.

[0436] Also, the secure container preparation unit 118 reads out the key file KF corresponding to the content data C from the key file database 118b and outputs this to the signature processing unit 117.

[0437] Then, the signature processing unit 117 obtains the hash value of the key file KF input from the secure container preparation unit 118, produces the signature data $SIG_{7,CP}$ by using the secret key data $K_{CP,S}$, and outputs this to the secure container preparation unit 118.

[0438] Next, the secure container preparation unit 118 produces the secure container 104 storing the content file CF and the signature data $SIG_{6,CP}$ thereof shown in Fig. 5A, the key file KF and the signature data $SIG_{7,CP}$ thereof shown in Fig. 5B, and the certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof shown in Fig. 5C read out from the storage unit 119 therein and stores this in the secure container database 118b. Then, the secure container preparation unit 118 reads out the secure container 104 to be provided to the user home network 103 in response to for example a request from the user from the secure container database 118a, encrypts this at the encryption and/or decryption unit 121 by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 120 and the SAM 105_1, and then transmits the same via the SAM management unit 124 to the SAM 105_1 of the user home network 103.

[0439] Below, a summary of the flow of the overall processing of the content provider 101 will be explained relative to the secure container preparation processing.

[0440] Figure 20, Fig. 21, and Fig. 22 are flowcharts for explaining the flow of the related processing.

[0441] Step B1: The content provider 101 receives as input its own certificate data CER_{CP} from the EMD service center 102 in advance and stores this in the storage unit (database) 119.

[0442] Step B2: The content data to be newly authored and an already stored content master source such as legacy content data are digitized, allocated a content ID, and stored in the content master source database 111 and uniquely managed.

[0443] Step B3: The meta data Meta is produced for each content master source uniquely managed at step B1 and is stored in the storage unit 119.

[0444] Step B4: The content data S111 serving as the content master source is read out from the content master source database 111 and output to the electronic watermark information addition unit 112, the electronic watermark information is buried, and the content data S112 is produced.

[0445] Step B5: The electronic watermark information addition unit 112 stores the content of the buried electronic watermark information and the burial location in the predetermined database.

[0446] Step B6: In the compression unit 113, the content data S112 with the electronic watermark information buried therein is compressed to produce the content data S113.

[0447] Step B7: In the expansion unit 116, the compressed content data S113 is expanded to produce the content data S116.

[0448] Step B8: In the audial check unit 123, the check of the sound of the expanded content data S116 is carried out.

[0449] Step B9: The content provider 101 detects the electronic watermark information buried in the content data S116 based on the buried content and the burial location stored in the database at step B5.

[0450] Then, the content provider 101 performs the processing of step B10 where both of the audial check

and the detection of the electronic watermark information succeed, while repeats the processing of step B4 where either one fails.

[0451] Step B10: A random number is generated at the random number generation unit 115 to produce the content key data Kc, and this is stored in the storage unit 119.

[0452] Step B11: In the encryption unit 114, the compressed content data S113 is encrypted by using the content key data Kc to produce the content data C.

[0453] Step B12: In the usage control policy data preparation unit 122, the usage control policy data 106 for the content data C is produced.

[0454] Step B13: The content provider 101 determines the SRP and stores this in the storage unit 119.

[0455] Step B14: The content provider 101 outputs the content ID, content key data Kc, and the usage control policy data 106 to the EMD service center 102.

[0456] Step B15: The content provider 101 receives as input the key file KF encrypted by the distribution use key data KD_1 to KD_3 from the EMD service center 102.

[0457] Step B16: The content provider 101 stores the input key file KF in the key file database 118b.

[0458] Step B17: The content provider 101 connects the links of the content data C and the key file KF by the hyper link.

[0459] Step B18: In the signature processing unit 117, the signature data indicating the legitimacy of the producer is produced by using the secret key data $K_{CP,S}$ for each of the content data C and the key files KF.

[0460] Step B19: In the secure container preparation unit 118, the secure container 104 shown in Fig. 5 is produced.

[0461] Step B20: Where the content data is provided in a composite form using a plurality of secure containers, the processing of the steps B1 to B19 is repeated to produce the secure container 104 and the link between the content file CF and the key file KF and the link among the content files CF by using the hyper link, etc.

[0462] Step B21: The content provider 101 stores the produced secure container 104 in the secure container database 118a.

[EMD service center 102]

[0463] The EMD service center 102 has a certificate authority (CA) function, a key management function., and a rights clearing (profit distribution) function.

[0464] Figure 23 is a view of the configurations of functions of the EMD service center 102.

[0465] As shown in Fig. 23, the EMD service center 102 has a key server 141, a key database 141a, a settlement processing unit 142, a signature processing unit 143, a settlement manager management unit 144, a certificate and/or usage control policy management unit 145, a usage control policy database 145a, a certificate database 145b, a content provider management unit 148, a CP database 148a, a SAM management unit 149, a SAM database 149a, a mutual certification unit 150, an encryption and/or decryption unit 151, and a KF preparation unit 153.

[0466] Note that, in Fig. 23, the flow of the data related to the data transmitted and received between the EMD service center 102 and the content provider 101 in the flow of the data among the functional blocks in the EMD service center 102 is shown.

[0467] Also, in Fig. 24, the flow of the data related to the data transmitted and received between the SAMs 105_1 to 105_4 and the settlement manager 91 shown in Fig. 1 in the flow of the data among the functional blocks in the EMD service center 102 is shown.

[0468] The key server 141 reads out six months' worth of the distribution use key data having the expiration date of one month stored in the key database 141a and outputs the same to the SAM management unit 149.

[0469] Also, other than the key database 141a distribution use key data KD, one series of key data for storing the key data such as the secret key data $K_{ESC,S}$ of the EMD service center 102, storage use key data K_{STR}, media key data K_{MED}, and the MAC key data K_{MAC} are stored.

[0470] The settlement processing unit 142 performs settlement processing based on the usage log data 108 input from the SAMs 105_1 to 105_4, the suggested retailer's price SRP input from the certificate and/or usage control policy management unit 145 and sales price, produces the settlement report data 107 and settlement claim data 152, outputs the settlement report data 107 to the content provider management unit 148, and outputs the settlement claim data 152 to the settlement manager management unit 144.

[0471] Note that, the settlement processing unit 142 monitors whether or not transactions based on an illegal dumping price were carried out based on the sales price.

[0472] Here, the usage log data 108 indicates the log of the purchase and usage (reproduction, recording, transfer, etc.) of the secure container 104 in the user home network 103 and is used when determining the payment sum of a license fee related to the secure container 104 in the settlement processing unit 142.

[0473] In the usage log data 108, for example the content ID serving as the identifier of the content data C stored in the secure container 104, the identifier CP_ID of the content provider 101 distributing the secure container 104, the compression method of the content data C in the secure container 104, an identifier Media_ID of the storage medium storing the secure container 104, the identifier SAM_ID of the SAMs 105_1 to 105_4 receiving the distribution of the secure container 104, USER_ID of the user of the related SAMs 105_1 to 105_4, etc. are described. Accordingly, the EMD service center 102 determines the sum of payment for each other party based on a distribution rate table determined in advance when it is necessary to distribute the money paid by the user of the user home network 103 to license owners of for example the compression method and the storage

medium other than the owner of the content provider 101 and produces the settlement report data 107 and the settlement claim data 152 in accordance with the related determination. The related distribution rate table is produced for example for every content data stored in the secure container 104.

[0474] Also, the settlement claim data 152 is the authenticated data for which the payment of money to the settlement manager 91 may be claimed. For example, when the money paid by the user is distributed to a plurality of right holders, it is produced for individual right holders.

[0475] Note that, the settlement manager 91 sends a statement of the related settlement manager to the EMD service center 102 when the settlement is terminated. The EMD service center 102 notifies the content of the related statement to the corresponding right holders.

[0476] The settlement manager management unit 144 transmits the settlement claim data 152 produced by the settlement processing unit 142 via the payment gateway 90 shown in Fig. 1 to the settlement manager 91.

[0477] Note that, as will be mentioned later, it is also possible if the settlement manager management unit 144 transmits the settlement claim data 152 to the right holders of the content provider 101 etc., and the right holders per se perform the settlement at the settlement manager 91 by using the received settlement claim data 152.

[0478] Also, the settlement manager management unit 144 obtains the hash value of the settlement claim data 152 in the signature processing unit 143 and transmits signature data SIG_{99} produced by using the secret key data $K_{ESC,S}$ together with the settlement claim data 152 to the settlement manager 91.

[0479] The certificate and/or usage control policy management unit 145 reads out the certificate data CER_{CP} and certificate data CER_{SAM1} to CER_{SAM4} etc. which are registered (stored) in the certificate database 145b and authenticated and, at the same time, registers the usage control policy data 106 of the content provider 101, the content key data Kc, the watermark module WM, etc. in the usage control policy database 145a to authenticate the same.

[0480] Here, for the usage control policy database 145a, a search is carried out by using the content ID as a search key, while for the certificate database 145b, a search is carried out by using the identifier CP_ID of the content provider 101 as the search key.

[0481] Also, the certificate and/or usage control policy management unit 145 obtains the hash values of for example the usage control policy data 106, content key data Kc, and the watermark module WM and stores the authenticated data attached with the signature data using the secret key data $K_{ESC,S}$ in the usage control policy database 145a.

[0482] The content provider management unit 148 has a function of communication with the content provider 101 and can access the CP database 148a for managing the identifiers CP_ID etc. of the registered content providers 101.

[0483] The SAM management unit 149 has a function of communication with the SAMs 105_1 to 105_4 in the user home network 103 and can access the SAM database 149a storing the identifiers SAM_ID and SAM registration list etc. of the registered SAMs.

[0484] The KF preparation unit 153 outputs the content key data Kc and usage control policy data 106 input from the content provider management unit 148 and the SAM program download containers SDC_1 to SDC_3 to the signature processing unit 143.

[0485] Also, the KF preparation unit 153 encrypts the content key data Kc, the usage control policy data 106, and the SAM program download containers SDC_1 to SDC_3 by using the distribution use key data KD_1 to KD_6 of the corresponding period input from the key server 141, produces the key file KF storing the related encrypted data and the signature data $SIG_{K1,ESC}$ by the secret key data $K_{ESC,S}$ for the related encrypted data input from the signature processing unit 143 therein as shown in Fig. 5B, and stores the related produced key file KF in the KF database 153a.

[0486] Below, an explanation will be given of the flow of the processing in the EMD service center 102.

[0487] First, an explanation will be given of the flow of the processing when transmitting the distribution use key data from the EMD service center 102 to the SAMs 105_1 to 105_4 in the user home network 103 by referring to Fig. 24.

[0488] As shown in Fig. 24, the key server 141 reads out for example three months' worth of the distribution use key data KD_1 to KD_3 from the key database 141a every predetermined period and outputs the same to the SAM management unit 149.

[0489] Also, the signature processing unit 143 obtains the hash values of each of the distribution use key data KD_1 to KD_3 to produce signature data $SIG_{KD1,ESC}$ to $SIG_{KD3,ESC}$ individually corresponding to them by using the secret key data $K_{ESC,S}$ of the EMD service center 102 and outputs them to the SAM management unit 149.

[0490] The SAM management unit 149 encrypts these three months' worth of the distribution use key data KD_1 to KD_3 and the signature data $SIG_{KD1,ESC}$ to $SIG_{KD3,ESC}$ of them by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the SAMs 105_1 to 105_4 and then transmits them to the SAMs 105_1 to 105_4.

[0491] Next, an explanation will be given of the processing in the case where the EMD service center 102 receives an issuance request of the certificate data CER_{CP} from the content provider 101 by referring to Fig. 23.

[0492] In this case, when receiving the identifier CP_ID of the content provider 101, public key data $K_{CP,P}$, and the signature data $SIG_{9,CP}$ from the content provider 101, the content provider management unit 148

decrypts them by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4.

[0493] Then, after confirming the legitimacy of the related decrypted signature data $SIG_{9,CP}$ at the signature processing unit 143, it is confirmed whether or not the content provider 101 issuing the issuance request of the related certificate data is registered in the CP database 148a based on the identifier CP_ID and the public key data $K_{CP,P}$.

[0494] Then, the certificate and/or usage control policy management unit 145 reads out the certificate data CER_{CP} of the related content provider 101 from the certificate database 145b and outputs this to the content provider management unit 148.

[0495] Also, the signature processing unit 143 obtains the hash value of the certificate data CER_{CP}, produces the signature data $SIG_{1,ESC}$ by using the secret key data $K_{ESC,S}$ of the EMD service center 102, and outputs this to the content provider management unit 148.

[0496] Then, the content provider management unit 148 encrypts the certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4 and then transmits the same to the content provider 101.

[0497] Next, an explanation will be given of the processing where the EMD service center 102 receives the issuance request of the certificate data CER_{SAM1} from the SAM 105_1 by referring to Fig. 24.

[0498] In this case, when receiving an identifier SAM_1_ID of the SAM 105_1, public key data $K_{SAM1,P}$, and signature data $SIG_{8,SAM1}$ from the SAM 105_1, the SAM management unit 149 decrypts them by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the SAM 105_1.

[0499] Then, after confirming the legitimacy of the related decrypted signature data $SIG_{8,SAM1}$ in the signature processing unit 143, based on the identifier SAM_1_ID and the public key data $K_{SAM1,P}$, it is confirmed whether or not the SAM 105_1 outputting the issuance request of the related certificate data is registered in the SAM database 149a.

[0500] Then, the certificate and/or usage control policy management unit 145 reads out the certificate data CER_{SAM1} of the related SAM 105_1 from the certificate database 145b and outputs this to the SAM management unit 149.

[0501] Also, the signature processing unit 143 obtains the hash value of the certificate data CER_{SAM1}, produces signature data $SIG_{50,ESC}$ by using the secret key data $K_{ESC,S}$ of the EMD service center 102, and outputs this to the SAM management unit 149.

[0502] Then, the SAM management unit 149 encrypts the certificate data CER_{SAM1} and the signature data $SIG_{50,ESC}$ thereof by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the SAM 105_1, and then transmits the same to the SAM 105_1.

[0503] Note that, the processing where the SAMs 105_1 to 105_4 request the certificate data is the same as the case of the SAM 105_1 mentioned above except only the object is replaced by the SAMs 105_1 to 105_4.

[0504] Note that, in the present invention, it is also possible if the EMD service center 102 produces the certificate data CER_{SAM1} of the public key data $K_{SAM1,P}$ at the time of shipment when a secret key data $K_{SAM1,S}$ and the public key data $K_{SAM1,P}$ of the SAM 105_1 are stored in the storage unit of the SAM 105_1 at for example the related shipment of the SAM 105_1.

[0505] At this time, at the related shipment, it is also possible to store the certificate data CER_{SAM1} in the storage unit of the SAM 105_1.

[0506] Next, an explanation will be given of the processing where the EMD service center 102 receives the registration use module Mod_2 shown in Fig. 1 from the content provider 101 by referring to Fig. 23.

[0507] In this case, when the content provider management unit 148 receives the registration use module Mod_2 shown in Fig. 18 from the content provider 101, the registration use module Mod_2 is decrypted by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4.

[0508] Then, in the signature processing unit 143, the legitimacy of the signature data $SIG_{M1,CP}$ is verified by using the public key data $K_{CP,P}$ read out from the key database 141a.

[0509] Next, the certificate and/or usage control policy management unit 145 registers the usage control policy data 106, content key data Kc, watermark module WM, and SRP stored in the registration use module Mod_2 in the usage control policy database 145a.

[0510] Next, the content provider management unit 148 outputs the content key data Kc and the usage control policy data 106 to the KF preparation unit 153.

[0511] Next, the KF preparation unit 153 outputs the content key data Kc and usage control policy data 106 input from the content provider management unit 148 and the SAM program download containers SDC_1 to SDC_3 to the signature processing unit 143.

[0512] Then, the signature processing unit 143 obtains the hash value with respect to the whole data input from the KF preparation unit 153, produces the signature data $SIG_{K1,ESC}$ thereof by using the secret key data $K_{ESC,S}$ of the EMD service center 102, and outputs this to the KF preparation unit 153.

[0513] Next, in the KF preparation unit 153, by using the distribution use key data KD_1 to KD_6 of the corresponding period input from the key server 141, the content key data Kc and usage control policy data 106 and the SAM program download containers SDC_1 to SDC_3 are encrypted, and the key file KF storing the related

encrypted data and the signature data $SIG_{K1,ESC}$ input from the signature processing unit 143 therein is produced and is stored in the KF database 153a.

[0514] Here, as the SAM program download containers SDC_1 to SDC_3, it is also possible to use those stored in the registration use module Mod_2 or it is also possible to use those held by the EMD service center 102 in advance.

[0515] Next, the content provider management unit 148 encrypts the key file KF obtained by accessing the KF database 153a by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4, and then transmits the same to the content provider 101.

[0516] Next, an explanation will be given of the settlement processing performed in the EMD service center 102 by referring to Fig. 24.

[0517] When receiving as input the usage log data 108 and signature data $SIG_{200,SAM1}$ thereof from for example the SAM 105_1 of the user home network 103, the SAM management unit 149 decrypts the usage log data 108 and the signature data $SIG_{200,SAM1}$ by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the SAM 105_1, verifies the signature data $SIG_{200,SAM1}$ by the public key data K_{SAM1} of the SAM 105_1, and then outputs the same to the settlement processing unit 142.

[0518] Then, the settlement processing unit 142 performs the settlement processing based on the usage log data 108 input from the SAM management unit 149 and the suggested retailer's price SRP contained in the usage control policy data 106 read out from the usage control policy database 145a via the certificate and/or usage control policy management unit 145 and the sales price and produces the settlement claim data 152 and the settlement report data 107.

[0519] The settlement processing unit 142 outputs the settlement claim data 152 to the settlement manager management unit 144 and, at the same time, outputs the settlement report data 107 to the content provider management unit 148.

[0520] Next, the settlement manager management unit 144 transmits the settlement claim data 152 and the signature data SIG_{99} thereof via the payment gateway 90 shown in Fig. 1 to the settlement manager 91 after the mutual certification and the decryption by the session key data K_{SES}.

[0521] By this, the money of the sum indicated in the settlement claim data 152 is paid to the content provider 101.

[0522] Next, an explanation will be given of the processing where the EMD service center 102 transmits the settlement report to the content provider 101 by referring to Fig. 23.

[0523] When the settlement is carried out in the settlement processing unit 142, as mentioned above, the settlement report data 107 is output from the settlement processing unit 142 to the content provider management unit 148.

[0524] In the settlement report data 107, as mentioned above, for example the content of the settlement concerning the content provider 101 performed with respect to the settlement manager 91 shown in Fig. 1 by the EMD service center 102 is described.

[0525] When receiving as input the settlement report data 107 from the settlement processing unit 142, the EMD service center 102 encrypts this by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4 and then transmits the same to the content provider 101.

[0526] Also, after registering (authenticating) the usage control policy data 106 as mentioned above, the EMD service center 102 may encrypt the authenticated certificate module by the distribution use key data KD_1 to KD_6 and transmit the same from the EMD service center 102 to the content provider 101 too.

[0527] Also, the EMD service center 102 performs the processing at the time of shipment of the SAMs 105_1 to 105_4 and the registration processing of the SAM registration list other than the above, but these processings will be mentioned later.

[User home network 103]

[0528] The user home network 103 has a network apparatus 160_1 and A/V apparatuses 160_2 to 160_4 as shown in Fig. 1.

[0529] The network apparatus 160_1 includes a built-in SAM 105_1. Also, the AV apparatuses 160_2 to 160_4 includes built-in SAMs 105_2 to 105_4.

[0530] The SAMs 105_1 to 105_4 are connected to each other via a bus 191, for example, an IEEE1394 serial interface bus.

[0531] Note that, the AV apparatuses 160_2 to 160_4 can have a network communication function too or may not have the network communication function, but utilize the network communication function of the network apparatus 160_1 via the bus 191.

[0532] Also, the user home network 103 can have only AV apparatuses not having the network function too.

[0533] Below, an explanation will be made of the network apparatus 160_1.

[0534] Figure 25 is a view of the configuration of the network apparatus 160_1.

[0535] As shown in Fig. 25, the network apparatus 160_1 has the SAM 105_1, a communication module 162, a decryption and/or expansion module 163, a purchase and/or usage form determination operation unit 165, a download memory 167, a reproduction module 169, and an external memory 201.

[0536] The SAMs 105_1 to 105_4 are modules for performing the charge processing in units of content and communicate with the EMD service center 102.

[0537] The SAMs 105_1 to 105_4 are managed in their

specifications, versions, etc. by for example the EMD service center 102. If there is a desire for mounting them by a home electric apparatus maker, they are licensed as a black box charging module for charging in units of content. For example, a home electric apparatus developer/manufacturer cannot determine the specifications inside the ICs (integrated circuits) of the SAMs 105_1 to 105_4. The EMD service center 102 standardizes the interfaces etc. of the related ICs. They are mounted in the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4 according to that.

[0538] The SAMs 105_1 to 105_4 are hardware modules (IC modules etc.) having tamper resistance so that the processing contents thereof are completely sheltered from the outside, the processing contents cannot be monitored or tampered with from the outside, and the data stored inside in advance and the data being processed cannot be monitored and tampered with from the outside.

[0539] When the functions of the SAMs 105_1 to 105_4 are realized in the form of ICs, secret memories are provided inside the ICs, and secret programs and secret data are stored there. If the function of a SAM can be incorporated in any other portion of the apparatus not limited to the physical form of an IC, that portion can be defined as a SAM too.

[0540] Below, a detailed explanation will be made of the function of the SAM 105_1.

[0541] Note that the SAMs 105_2 to 105_4 have basically the same functions as the SAM 105_1.

[0542] Figure 26 is a view of the configuration of the function of the SAM 105_1.

[0543] Note that, in Fig. 26, the flow of the data related the processing of inputting a secure container 104 from the content provider 101 and decrypting the key file KF in the secure container 104 is shown.

[0544] As shown in Fig. 26, the SAM 105_1 has a mutual certification unit 170, encryption and/or decryption units 171, 172, and 173, a content provider management unit 180, an error correction unit 181, a download memory management unit 182, a secure container decryption unit 183, a decryption and/or expansion module management unit 184, an EMD service center management unit 185, a usage monitor unit 186, a charge processing unit 187, a signature processing unit 189, a SAM management unit 190, a media SAM management unit 197, a stack (work) memory 200, and an external memory management unit 811.

[0545] Note that, the AV apparatuses 160_2 to 160_4 do not have the download memory 167, so the download memory management unit 182 does not exist in the SAM 105_2 to 105_4.

[0546] Note that, the predetermined function of the SAM 105_1 shown in Fig. 26 is realized by executing a secret program in for example a not illustrated CPU.

[0547] Also, in the external memory 201, after going through the following processing, as shown in Fig. 27, a usage log data 108 and a SAM registration list are stored.

[0548] Here, the memory space of the external memory 201 cannot be seen from the outside (for example a host CPU 810) of the SAM 105_1. Only the SAM 105_1 can manage access with respect to the storage region of the external memory 201.

[0549] As the external memory 210, use is made of for example a flash memory or a ferro-electric memory (FeRAM).

[0550] Also, as the stack memory 200, use is made of for example a SARAM. As shown in Fig. 28, the secure container 104, content key data Kc, usage control policy data (UCP) 106, a lock key data K_{LOC} of a storage unit 192, certificate data CER_{CP} of the content provider 101, usage control status data (UCS) 166, SAM program download containers SDC_1 to SDC_3, etc. are provided.

[0551] Below, among the functions of the SAM 105_1, the processing contents of the functional blocks when the secure container 104 from the content provider 101 is input will be explained by referring to Fig. 26.

[0552] The mutual certification unit 170 performs mutual certification between the content provider 101 and the EMD service center 102 when the SAM 105_1 transmits and receives the data on-line between the content provider 101 and the EMD service center 102 to produce a session key data (common key) K_{SES} and outputs this to the encryption and/or decryption unit 171. The session key data K_{SES} is newly produced with each mutual certification.

[0553] The encryption and/or decryption unit 171 encrypts and/or decrypts the data transmitted and received between the content provider 101 and the EMD service center 102 by using the session key data K_{SES} produced by the mutual certification unit 170.

[0554] The error correction unit 181 corrects the error of the secure container 104 and outputs the same to the download memory management unit 182.

[0555] Note that, it is also possible if the user home network 103 has a function for detecting whether or not the secure container 104 has been tampered with.

[0556] In the present embodiment, the case where the error correction unit 181 was built in the SAM 105_1 was exemplified, but it is also possible to impart the function of the error correction unit 181 to the outside of the SAM 105_1, for example, the host CPU 810.

[0557] The download memory management unit 182 performs the mutual certification between the mutual certification unit 170 and a media SAM 167a in a case where the download memory 167 has a media SAM 167a having a mutual certification function as shown in Fig. 25, and then encrypts the secure container 104 after the error correction by using the session key data K_{SES} obtained by the mutual certification and writes the same into the download memory 167 shown in Fig. 25. As the download memory 167, use is made of for example a nonvolatile semiconductor memory such as memory stick.

[0558] Note that, as shown in Fig. 29, where a memory not provided with a mutual certification function such as a HDD (hard disk drive) is used as a download memory 211, the inside of the download memory 211 is not secure, so the content file CF is downloaded on the download memory 211, and a key file KF having a high secrecy is downloaded on for example the stack memory 200 shown in Fig. 26.

[0559] The secure container decryption unit 183 decrypts the content key data Kc, usage control policy data 106, and the SAM program download containers SDC_1 to SDC_3 in the key file KF stored in the secure container 104 input from the download memory management unit 182 by using distribution use key data KD_1 to KD_3 read out from the storage unit 192.

[0560] The related decrypted content key data Kc, usage control policy data 106, and the SAM program download containers SDC_1 to SDC_3 are written into the stack memory 200.

[0561] The EMD service center management unit 185 manages the communication with the EMD service center 102 shown in Fig. 1.

[0562] The signature processing unit 189 verifies the signature data in the secure container 104 by using a public key data $K_{ESC,P}$ of the EMD service center 102 read out from the storage unit 192 and the public key data $K_{CP,P}$ of the content provider 101.

[0563] The storage unit 192 stores, as the secret data which cannot be read out and rewritten from the outside of the SAM 105_1, as shown in Fig. 30, a plurality of distribution use key data KD_1 to KD_3 with expiration dates, SAM_IDs, user IDs, passwords, information reference use IDs, a SAM registration list, storage use key data K_{STR}, public key data $K_{R\text{-}CA,P}$ of the route CA, public key data $K_{ESC,P}$ of the EMD service center 102, media key data K_{MED}, public key data $K_{ESC,P}$ of the EMD service center 102, secret key data $K_{SAM1,S}$ of the SAM 105_1, the certificate data CER_{SAM1} storing public key data $K_{SAM1,P}$ of the SAM 105_1 therein, signature data SIG_{22} of the certificate CER_{ESC} using the secret key data $K_{ESC,S}$ of the EMD service center 102, the original key data for the mutual certification with the decryption and/or expansion module 163 (where the common key encryption method is employed), the original key data for the mutual certification with the media SAM (where the common key encryption method is employed), and certificate data CER_{MEDSAM} of the media SAM (where the public key encryption method is employed).

[0564] Also, in the storage unit 192, a secret program for realizing at least one part of the functions shown in Fig. 26 is stored.

[0565] As the storage unit 192, use is made of for example a flash-EEPROM (electrically erasable programmable RAM).

[0566] Below, an explanation will be made of the flow of the processing in the SAM 105_1 when storing the distribution use key data KD_1 to KD_3 received from the EMD service center 102 in the storage unit 192 by referring to Fig. 26.

[0567] In this case, first, mutual certification is carried out between the mutual certification unit 170 and the mutual certification unit 150 shown in Fig. 23.

[0568] Next, three months' worth of the distribution use key data K_1 to K_3 encrypted by the session key data K_{SES} obtained by the related mutual certification and the signature data $SIG_{KD1,ESC}$ to$SIG_{KD3,ESC}$ thereof are written from the EMD service center 102 via the EMD service center management unit 185 into the stack memory 811.

[0569] Next, in the encryption and/or decryption unit 171, by using the session key data K_{SES}, the distribution use key data K_1 to K_3 and the signature data $SIG_{KD1,ESC}$ to$SIG_{KD3,ESC}$ thereof are decrypted.

[0570] Next, in the signature processing unit 189, after the legitimacy of the signature data $SIG_{KD1,ESC}$ to $SIG_{KD3,ESC}$ stored in the stack memory 811 is confirmed, the distribution use key data K_1 to K_3 are written into the storage unit 192.

[0571] Below, an explanation will be made of the flow of the processing in the SAM 105_1 receiving as input the secure container 104 provided by the content provider 101 by referring to Fig. 26.

[0572] Mutual certification is carried out between the mutual certification unit 170 of the SAM 105_1 shown in Fig. 26 and the mutual certification unit 120 shown in Fig. 3.

[0573] The encryption and/or decryption unit 171 decrypts the secure container 104 supplied from the content provider 101 via the content provider management unit 180 by using the session key data K_{SES} obtained by the related mutual certification.

[0574] Next, the signature processing unit 189 verifies the signature data $SIG_{1,ESC}$ shown in Fig. 5C and then verifies the legitimacy of the signature data $SIG_{6,CP}$ and $SIG_{7,CP}$ by using the public key data $K_{CP,P}$ of the content provider 101 stored in the certificate data CER_{CP} shown in Fig. 5C.

[0575] At this time, when it is verified that the signature data $SIG_{6,CP}$ is legitimate, the legitimacy of the producer and the transmitter of the content file CF is confirmed.

[0576] Also, when it is verified that the signature data $SIG_{7,CP}$ is legitimate, the legitimacy of the transmitter of the key file KF is confirmed.

[0577] Also, the signature processing unit 189 verifies the legitimacy of the signature data $SIG_{K1,ESC}$ in the key file KF shown in Fig. 5B, that is, the legitimacy of the producer of the key file KF and whether or not the key file KF is registered in the EMD service center 102 by using the public key data $K_{ESC,P}$ read out from the storage unit 192.

[0578] The content provider management unit 180 outputs the secure container 104 to the error correction unit 181 when the legitimacy of the signature data $SIG_{6,CP}$, $SIG_{7,CP}$, and $SIG_{K1,ESC}$ is confirmed.

[0579] The error correction unit 181 performs the error

correction of the secure container 104 and then outputs the same to the download memory management unit 182.

[0580] The download memory management unit 182 writes the secure container 104 into the download memory 167 after performing the mutual certification between the mutual certification unit 170 and the media SAM 167a shown in Fig. 25.

[0581] Next, the download memory management unit 182 performs mutual certification between the mutual certification unit 170 and the media SAM 167a shown in Fig. 25 and then reads out the key file KF shown in Fig. 5B stored in the secure container 104 from the download memory 167 and outputs the same to the secure container decryption unit 183.

[0582] Then, in the secure container decryption unit 183, by using the distribution use data KD_1 to KD_3 of the corresponding period input from the storage unit 192, the content key data Kc, usage control policy data 106, and the SAM program download containers SDC_1 to SDC_3 in the key file KF shown in Fig. 5Bare decrypted.

[0583] Then, the decrypted content key data Kc, usage control policy data 106, and the SAM program download containers SDC_1 to SDC_3 are written into the stack memory 200.

[0584] Below, an explanation will be made of the processing contents of the functional blocks related to the processing of using and purchasing the content data C downloaded on the download memory 167 by referring to Fig. 31.

[0585] The usage monitor unit 186 reads out the usage control policy data 106 and the usage control status data 166 from the stack memory 200 and monitors so that the purchase and/or usage of the content is carried out within a range permitted by the related read out usage control policy data 106 and usage control status data 166.

[0586] Here, the usage control policy data 106 is stored in the KF after decryption and stored in the stack memory 200 as explained by using Fig. 26.

[0587] Also, the usage control status data 166 is stored in the stack memory 200 when the purchase form is determined by the user as will be mentioned later.

[0588] The charge processing unit 187 produces the usage log data 108 in response to an operation signal S165 from the purchase and/or usage form determination operation unit 165 shown in Fig. 25.

[0589] Here, the usage log data 108 describes the log of the purchase and usage forms of the secure container 104 by the user as mentioned before and is used when performing settlement processing in accordance with the purchase of the secure container 104 and determining the payment of the license fee in the EMD service center 102.

[0590] Also, the charge processing unit 187 notifies the sales price or the suggested retailer's price data SRP read out from the stack memory 200 to the user according to need.

[0591] Here, the sales price and the suggested retailer's price data SRP have been stored in the usage control policy data 106 of the key file KF shown in Fig. 5B stored in the stack memory 200 after decryption.

[0592] The charge processing by the charge processing unit 187 is carried out based on the right content such as the usage permission condition indicated by the usage control policy data 106 and the usage control status data 166 under the monitoring of the usage monitor unit 186. Namely, the user purchases and uses the content within the range according to the related right content, etc.

[0593] Also, the charge processing unit 187 produces the usage control status (UCS) data describing the purchase form of the content by the user and writes this into the stack memory 200.

[0594] As the purchase form of the content, there are for example an outright purchase without restriction as to the reproduction by the purchaser and copying for the usage of the related purchaser, a reproduction charge for charging with each reproduction, etc.

[0595] Here, the usage control status data 166 is produced when the user determines the purchase form of the content and is used for control so that the user uses the related content within the range permitted by the related determined purchase form Shereafter. In the usage control status data 166, the ID of the content, the purchase form, the price in accordance with the related purchase form, the SAM_ID of the SAM with the purchase of the related content performed therefor, the USER_ID of the purchased user, etc. are described.

[0596] Note that, where the determined purchase form is a reproduction charge, for example, the usage control status data 166 is transmitted from the $SAM\ 105_1$ to the content provider 101 in real-time simultaneously with the purchase of the content data C, and the content provider 101 instructs the EMD service center 102 to obtain the usage log data 108 at the $SAM\ 105_1$ within the predetermined period.

[0597] Also, where the determined purchase form is an outright purchase, for example, the usage control status data 166 is transmitted in real-time to both of the content provider 101 and the EMD service center 102. In this way, in the present embodiment, in both cases, the usage control status data 166 is transmitted in real-time to the content provider 101.

[0598] The EMD service center management unit 185 transmits the usage log data 108 read out from the external memory 201 via the external memory management unit 811 to the EMD service center 102.

[0599] At this time, the EMD service center management unit 185 produces the signature data $SIG_{200,SAM1}$ of the usage log data 108 by using the secret key data $K_{SAM1,S}$ in the signature processing unit 189 and transmits the signature data $SIG_{200,SAM1}$ together with the usage log data 108 to the EMD service center 102.

[0600] The usage log data 108 can be transmitted to the EMD service center 102 in response to for example

a request from the EMD service center 102 or periodically or can be transmitted when the amount of information of the log information contained in the usage log data 108 becomes a predetermined amount or more too. The related amount of information is determined in accordance with for example the storage capacity of the external memory 201.

[0601] The download memory management unit 182 outputs the content data C read out from the download memory 167, content key data Kc read out from the stack memory 200, and the user watermark use data 196 input from the charge processing unit 187 to the decryption and/or expansion module management unit 184 in the case where for example a reproduction operation of the content is carried out in response to the operation signal S165 from the purchase form determination operation unit 165 shown in Fig. 25.

[0602] Also, the decryption and/or expansion module management unit 184 outputs the content file CF read out from the download memory 167 and the content key data Kc and a half disclosure parameter data 199 read out from the stack memory 200 to the decryption and/or expansion module management unit 184 when a demo operation of the content is carried out in response to the operation signal S165 from the purchase form determination operation unit 165 shown in Fig. 25.

[0603] Here, the half disclosure parameter data 199 is described in the usage control policy data 106 and indicates the handling of the content in the demo mode. In the decryption and/or expansion module 163, it becomes possible to reproduce the encrypted content data C in the half disclosure state based on the half disclosure parameter data 199. As the procedure of the half disclosure, there is for example a procedure of designating the blocks to be decrypted and the blocks not to be decrypted by using the content key data Kc, limiting the reproduction function at the demo or limiting a demo enable period by the half disclosure parameter data 199 by utilizing the fact that the decryption and/or expansion module 163 processes the data (signal) in units of predetermined blocks.

[0604] Below, an explanation will be made of the flow of the processing in the SAM 105_1.

[0605] First, an explanation will be made of the flow of the processing up to when the purchase form of the secure container 104 downloaded on the download memory 167 from the content provider 101 is determined by referring to Fig. 31.

[0606] When the operation signal S165 indicating the demo mode is output to the charge processing unit 187 by the operation of the purchase and/or usage form determination operation unit 165 shown in Fig. 25 by the user, for example, the content file CF stored in the download memory 167 is output via the decryption and/or expansion module management unit 184 to the decryption and/or expansion module 163 shown in Fig. 25.

[0607] At this time, for the content file CF, mutual certification between the mutual certification unit 170 and the media SAM 167a, encryption and/or decryption by the session key data K_{SES}, mutual certification between the mutual certification unit 170 and the mutual certification unit 220, and encryption and/or decryption by the session key data K_{SES} are carried out.

[0608] The content file CF is decrypted by using the session key data K_{SES} at the decryption unit 221 shown in Fig. 25, and then output to the decryption unit 222.

[0609] Also, the content key data Kc and the half disclosure parameter data 199 read out from the stack memory 200 are output to the decryption and/or expansion module 163 shown in Fig. 25. At this time, after the mutual certification between the mutual certification unit 170 and the mutual certification unit 220, encryption and decryption by the session key data K_{SES} are carried out with respect to the content key data Kc and the half disclosure parameter data 199.

[0610] Next, the decrypted half disclosure parameter data 199 is output to the half disclosure processing unit 225. Under the control of the half disclosure processing unit 225, the decryption of the content data C using the content key data Kc by the decryption unit 222 is carried out in half disclosure.

[0611] Next, the content data C decrypted in half disclosure is expanded at the expansion unit 223 and then output to the electronic watermark information processing unit 224.

[0612] Next, the user watermark use data 196 is buried in the content data C in the electronic watermark information processing unit 224, and then the content data C is reproduced at the reproduction module 169, and sound in accordance with the content data C is output.

[0613] Then, when the user trying out the content determines the purchase form by operating the purchase and/or usage form determination operation unit 165, the operation signal S165 indicating the related determined purchase form is output to the charge processing unit 187.

[0614] Then, in the charge processing unit 187, the usage log data 108 and the usage control status data 166 in accordance with the determined purchase form are produced, the usage log data 108 is written into the external memory 201 via the external memory management unit 811, and, at the same time, the usage control status data 166 is written into the stack memory 200.

[0615] Thereafter, in the usage monitor unit 186, control (monitoring) is carried out so that the content data is purchased and used within the range permitted by the usage control status data 166.

[0616] Then, a new key file KF_1 shown in Fig. 34C mentioned later is produced, and the related produced key file KF_1 is stored in the download memory 167 via the download memory management unit 182.

[0617] As shown in Fig. 34C, the usage control status data 166 stored in the key file KF_1 is sequentially encrypted by using the storage key data K_{STR} and the media key data K_{MED} by utilizing the CBC mode of the DES.

[0618] Here, the storage use key data K_{STR} is data

determined in accordance with the type of apparatus, for example, a SACD (Super Audio Compact Disc), a DVD (Digital Versatile Disc) apparatus, CD-R apparatus, and MD (Mini Disc) apparatus and is used for establishing one-to-one correspondence between the types of the apparatuses and the types of the storage media. Also, the media key data K_{MED} is data unique to the storage medium.

[0619] Also, in the signature processing unit 189, a hash value H_{K1} of the key file KF_1 is produced by using the secret key data $K_{SAM1,S}$ of the SAM 105_1, and the related produced hash value H_{K1} is written into the stack memory 200 in correspondence to the key file KF_1. The hash value H_{K1} is used for verifying the legitimacy of the producer of the key file KF_1 and whether or not the key file KF_1 was tampered with.

[0620] Next, the flow of the processing where the content data C with the purchase form already determined therefor stored in the download memory 167 will be explained by referring to Fig. 31.

[0621] In this case, under the monitoring of the usage monitor unit 186, based on the operation signal S165, the content file CF stored in the download memory 167 is output to the decryption and/or expansion module 163 shown in Fig. 31. At this time, mutual certification is carried out between the mutual certification unit 170 shown in Fig. 31 and the mutual certification unit 220 of the decryption and/or expansion module 163 shown in Fig. 25.

[0622] Also, the content key data Kc read out from the stack memory 200 is output to the decryption and/or expansion module 163.

[0623] Then, in the decryption unit 222 of the decryption and/or expansion module 163, the decryption of the content file CF using the content key data Kc and the expansion processing by an expansion unit 223 are carried out, and in the reproduction module 169, the content data C is reproduced.

[0624] At this time, by the charge processing unit 187, the usage log data 108 stored in the external memory 201 is updated in accordance with the operation signal S165.

[0625] The usage log data 108 is read out from the external memory 201, and then, after passing through the mutual certification, transmitted via the EMD service center management unit 185 together with the signature data $SIG_{200,SAM1}$ to the EMD service center 102.

[0626] Next, as shown in Fig. 32, the flow of the processing in the SAM 105_1 in a case where for example, after the purchase form of the content file CF downloaded on the download memory 167 of the network apparatus 160_1 is determined as mentioned above, a new secure container 104x storing the related content file CF is produced, and the secure container 104x is transferred via the bus 191 to the SAM 105_2 of the AV apparatus 160_2 will be explained by referring to Fig. 33.

[0627] The user operates the purchase and/or usage form determination operation unit 165 and instructs the transfer of the predetermined content stored in the download memory 167 to the AV apparatus 160_2, and the operation signal S165 in accordance with the related operation is output to the charge processing unit 187.

[0628] By this, the charge processing unit 187 updates the usage log data 108 stored in the external memory 201 based on the operation signal S165.

[0629] Also, the charge processing unit 187 transmits the usage control status data 166 indicating the related determined purchase form via the EMD service center management unit 185 to the EMD service center 102 whenever the purchase form of the content data is determined.

[0630] Also, the download memory management unit 182 outputs the content file CF and the signature data $SIG_{6,CP}$ thereof shown in Fig. 5A, the key file KF and the signature data $SIG_{7,CP}$ thereof, and the key file KF_1 and the hash value H_{K1} thereof read out from the download memory 167 to the SAM management unit 190. At this time, the mutual certification between the mutual certification unit 170 of the SAM 105_1 and the media SAM 167a and the encryption and/or decryption by the session key data K_{SES} are carried out.

[0631] Also, the signature processing unit 189 obtains the hash value of the content file CF, produces signature data $SIG_{41,SAM1}$ by using the secret key data $K_{SAM1,S}$, and outputs this to the SAM management unit 190.

[0632] Also, the signature processing unit 189 obtains the hash value of the key file KF_1, produces signature data $SIG_{42,SAM1}$ by using the secret key data $K_{SAM1,S}$, and outputs this to the SAM management unit 190.

[0633] Also, the SAM management unit 190 reads out the certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof and the certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof shown in Fig. 34D from the storage unit 192.

[0634] Also, the mutual certification unit 170 outputs the session key data K_{SES} obtained by performing the mutual certification with the SAM 105_2 to the encryption and/or decryption unit 171.

[0635] The SAM management unit 190 produces a new secure container 104x comprised of the data shown in Figs. 34A, 34B, 34C, and 34D, encrypts the secure container 104x in the encryption and/or decryption unit 171 by using the session key data K_{SES}, and then outputs the same to the SAM 105_2 of the AV apparatus 160_2 shown in Fig. 32.

[0636] At this time, in parallel to the mutual certification between the SAM 105_1 and the SAM 105_2, mutual certification of the bus 191 serving as the IEEE1394 serial bus is carried out.

[0637] Below, as shown in Fig. 32, the flow of the processing in the SAM 105_2 when writing the secure container 104x input from the SAM 105_1 into the storage medium 130_4 of a RAM type or the like will be explained by referring to Fig. 35.

[0638] Here, the RAM type storage medium 130_4 has for example an unsecure RAM region 134, a media SAM 133, and a secure RAM region 132.

[0639] In this case, the SAM management unit 190 of the SAM 105_2 receives as input the secure container 104x from the SAM 105_1 of the network apparatus 160_1 as shown in Fig. 32 and Fig. 35.

[0640] Then, in the encryption and/or decryption unit 171, the secure container 104x input via the SAM management unit 190 is decrypted by using the session key data K_{SES} obtained by the mutual certification between the mutual certification unit 170 and the mutual certification unit 170 of the SAM 105_1.

[0641] Next, in the signature processing unit 189, the legitimacy of the signature data $SIG_{6,CP}$ is verified by using the public key data $K_{CP,P}$, and the legitimacy of the producer of the content file CF is confirmed. Also, in the signature processing unit 189, the legitimacy of the signature data $SIG_{41,SAM1}$ is verified by using the public key data $K_{SAM1,P}$, and the legitimacy of the transmitter of the content file CF is confirmed.

[0642] Then, after it is confirmed that the producer and the transmitter of the content file CF are legitimate, the content file CF is output from the SAM management unit 190 to a storage module management unit 855, and the content file CF is written into the RAM region 134 of the RAM type storage medium 130_4 shown in Fig. 32.

[0643] Also, the key file KF and the signature data $SIG_{7,CP}$ and $SIG_{42,SAM1}$ thereof, the key file KF_1 and the hash value K_{K1} thereof, the certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof, and the certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof decrypted by using the session key data K_{SES} are written into the stack memory 200.

[0644] Next, the signature processing unit 189 verifies the signature data $SIG_{22,ESC}$ read out from the stack memory 200 by using the public key data $K_{ESC,P}$ read out from the storage unit 192 and confirms the legitimacy of the certificate data CER_{SAM1}.

[0645] Then, the signature processing unit 189 verifies the legitimacy of the signature data $SIG_{42,SAM1}$ stored in the stack memory 200 by using the public key data $K_{SAM1,P}$ stored in the certificate data CER_{SAM1} when confirming the legitimacy of the certificate data CER_{SAM1}. Then, when it is verified that the signature data $SIG_{42,SAM1}$ is legitimate, the legitimacy of the key file KF is confirmed.

[0646] Also, the signature processing unit 189 verifies the signature data $SIG_{1,ESC}$ read out from the stack memory 200 by using the public key data $K_{ESC,P}$ read out from the storage unit 192 and confirms the legitimacy of the certificate data CER_{CP}.

[0647] Then, the signature processing unit 189 verifies the legitimacy of the signature data $SIG_{7,SAM1}$ stored in the stack memory 200 by using the public key data $K_{CP,P}$ stored in the certificate data CER_{CP} when confirming the legitimacy of the certificate data CER_{CP}. Then, when it is verified that the signature data $SIG_{7,SAM1}$ is legitimate, the legitimacy of the producer of the key file KF is confirmed.

[0648] When it is confirmed that the producer and the transmitter of the key file KF are legitimate, the key file KF is read out from the stack memory 200 and written into the secure RAM region 132 of the RAM type storage medium 130_4 shown in Fig. 34 via the storage module management unit 855.

[0649] Also, the signature processing unit 189 verifies the legitimacy of the hash value H_{K1} by using the public key data $K_{SAM1,P}$ and confirms the legitimacy of the producer and transmitter of the key file KF_1.

[0650] Then, when the legitimacy of the producer and the transmitter of the key file KF_1 is confirmed, the key file KF_1 shown in Fig. 34C is read out from the stack memory 200 and output to the encryption and/or decryption unit 173.

[0651] Note that, in the related example, the case where the producer and the transmitter of the key file KF_1 were the same was mentioned, but where the producer and the transmitter of the key file KF_1 are different, the signature data of the producer and the signature data of the transmitter are produced with respect to the key file KF_1, and the legitimacy of the both signature data is verified in the signature processing unit 189.

[0652] Then, the encryption and/or decryption unit 173 encrypts the content key data Kc and the usage control status data 166 in the key file KF_1 by sequentially using the storage use key data K_{STR}, media key data K_{MED}, and the purchaser key data K_{PIN} read out from the storage unit 192 and outputs the same to the storage module management unit 855.

[0653] Then, by the storage module management unit 855, the encrypted key file KF_1 is stored in the secure RAM region 132 of the RAM type storage medium 130_4.

[0654] Note that, the media key data K_{MED} is stored in the storage unit 192 in advance by the mutual certification between the mutual certification unit 170 shown in Fig. 33 and the media SAM 133 of the RAM type storage medium 130_4 shown in Fig. 32.

[0655] Here, the storage use key data K_{STR} is data determined in accordance with the type of apparatus (AV apparatus 160_2 in the related example) of for example the SACD (Super Audio Compact Disc), DVD (Digital Versatile Disc) apparatus, CD-R apparatus, and MD (Mini Disc) apparatus and is used for establishing one-to-one correspondence between the types of the apparatuses and the types of the storage media. Note that, the physical structures of the disc media are the same between SACD and DVD, so there is a case where the recording and/or reproduction of the storage medium of an SACD can be carried out by using a DVD apparatus. The storage use key data K_{STR} performs the function of preventing illegitimate copies in such a case.

[0656] Note that, in the present embodiment, it is also possible not to encrypt using the storage use key data K_{STR}.

[0657] Also, the media key data K_{MED} is data unique to the storage medium (RAM type storage medium 130_4 in the related example).

[0658] The media key data K_{MED} is stored in the stor-

age medium (RAM type storage medium 130_4 shown in Fig. 32 in the related example). It is preferred from the viewpoint of the security that encryption and the decryption using the media key data K_{MED} be carried out in the media SAM of the storage medium. At this time, the media key data K_{MED} is stored in the related media SAM where the media SAM is mounted in the storage medium, while is stored in for example a region out of management of the host CPU 810 in the RAM region where the media SAM is not mounted in the storage medium.

[0659] Note that, it is also possible to perform the mutual certification between the apparatus side SAM (SAM 105_2 in the related example) and the media SAM (media SAM 133 in the related example), transfer the media key data K_{MED} via the secure communication route to the apparatus side SAM, and perform the encryption and decryption using the media key data K_{MED} in the apparatus side SAM as in the present embodiment.

[0660] In the present embodiment, the storage use key data K_{STR} and the media key data K_{MED} are used for protecting the security of the level of the physical layer of the storage medium.

[0661] Also, the purchaser key data K_{PIN} is data indicating the purchaser of the content file CF and is allocated by the EMD service center 102 to the related purchased user when for example the content is purchased by outright purchase. The purchaser key data K_{PIN} is managed in the EMD service center 102.

[0662] Also, in the above embodiment, the case where the key files KF and KF_1 were stored in the secure RAM region 132 of the RAM type storage medium 130_4 by using the storage module 260 was exemplified, but as indicated by a dotted line in Fig. 32, it is also possible to store the key files KF and KF_1 in the media SAM 133 from the SAM 105_2.

[0663] Next, the flow of the processing when determining the purchase form in the AV apparatus 160_2 where the user home network 303 is distributed the ROM type storage medium 130_1 shown in Fig. 12 with the purchase form of the content undetermined therefor off-line will be explained by referring to Fig. 36 and Fig. 37.

[0664] The SAM 105_2 of the AV apparatus 160_2 first performs the mutual certification between the mutual certification unit 170 shown in Fig. 37 and the media SAM 133 of the ROM type storage medium 130_1 shown in Fig. 12, and then receives as input the media key data K_{MED} from the media SAM 133.

[0665] Note that, where the SAM 105_2 holds the media key data K_{MED} in advance, it is also possible if the related input is not carried out.

[0666] Next, the key file KF and the signature data $SIG_{7,CP}$ thereof and the certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof shown in Figs. 5B and 5C stored in the secure container 104 stored in the secure RAM region 132 of the ROM type storage medium 130_1 are input via the media SAM management unit 197 or not illustrated read out module management unit and are written into the stack memory 200.

[0667] Next, in the signature processing unit 189, after the legitimacy of the signature data $SIG_{1,ESC}$ is confirmed, the public key data $K_{CP,P}$ is extracted from the certificate data CER_{CP}, and by using this public key data $K_{CP,P}$, the legitimacy of the signature data $SIG_{7,CP}$, that is, the legitimacy of the transmitter of the key file KF is verified.

[0668] Also, in the signature processing unit 189, by using the public key data $K_{ESC,P}$ read out from the storage unit 192, the legitimacy of the signature data $SIG_{K1,ESC}$ stored in the key file KF, that is, the legitimacy of the producer of the key file KF, is verified.

[0669] When the legitimacy of the signature data $SIG_{7,CP}$ and $SIG_{K1,ESC}$ is confirmed in the signature processing unit 189, the key file KF is read out from the stack memory 200 to the secure container decryption unit 183.

[0670] Next, in the secure container decryption unit 183, by using the distribution use data KD_1 to KD_3 of the corresponding period, the content key data Kc, usage control policy data 106, and the SAM program download containers SDC_1 to SDC_3 stored in the key file KF are decrypted and are written into the stack memory 200.

[0671] Next, after the mutual certification between the mutual certification unit 170 shown in Fig. 37 and the decryption and/or expansion module 163 shown in Fig. 36, the decryption and/or expansion module management unit 184 of the SAM 105_2 outputs the content key data Kc stored in the stack memory 200 and the half disclosure parameter data 199 stored in the usage control policy data 106 and the content data C stored in the content file CF read out from the ROM region 131 of the ROM type storage medium 130_1 to the decryption and/or expansion module 163 shown in Fig. 36. Next, in the decryption and/or expansion module 163, the content data C is decrypted in the half disclosure mode by using the content key data Kc and then expanded and output to a reproduction module 270. Then, in the reproduction module 270, the content data C from the decryption and/or expansion module 163 is reproduced.

[0672] Next, the purchase form of the content is determined by the purchase operation of the purchase form determination operation unit 165 shown in Fig. 36 by the user, and the operation signal S165 indicating the related determined purchase form is input to the charge processing unit 187.

[0673] Next, the charge processing unit 187 produces the usage control status data 166 in response to the operation signal S165 and writes this into the stack memory 200.

[0674] Next, the content key data Kc and the usage control status data 166 are output from the stack memory 200 to the encryption and/or decryption unit 173.

[0675] Next, the encryption and/or decryption unit 173 sequentially encrypts the content key data Kc and the usage control status data 166 input from the stack memory 200 by using the storage use key data K_{STR}, the me-